Toni Hietala

PALVELUJEN TURVAAMINEN KONESALIN PEILAUKSEN AVULLA

Tradenomi

Syksy 2015

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

TIIVISTELMÄ

Tekijä(t): Toni Hietala

Työn nimi: Palvelujen turvaaminen konesalin peilauksen avulla

Tutkintonimike: Tradenomi, tietojenkäsittely

Asiasanat: Peilaus, katastrofista palautuminen, Site Recovery Manager, replikointi

Opinnäytetyön tavoitteena oli toteuttaa ja testata ratkaisu konesalin peilaukseen, käyttäen VMwaren vCenter Site Recovery Manager -ohjelmistoa. Konesalit ovat usein alttiita erilaisille vaaroille, jotka voivat vahingoittaa niiden toimintaa tai ajaa ne alas, näin aiheuttaen taloudellista menetystä, jos tällaisten tilanteiden varalta ei ole valmistauduttu.

Opinnäytetyön tilaajana oli Kajaanin ammattikorkeakoulu, ja sen käytännön työ toteutettiin koulun tietojärjestelmälaboratoriossa. Työ kattaa ympäristön asennuksen ja testauksen vaiheet sekä aiheen taustalla olevan teorian.

Konesaliympäristöt virtualisoitiin ESXi-hypervisoreiden päälle. Virtuaaliympäristöjen hallintaan käytettiin vCenter Serveriä ja replikointiin vSphere Replicationia, molemmat appliance asennuksina. Testit saatiin suoritettua onnistuneesti ja turvattavat palvelut palautettua toimintaansa noin tunnissa pääsijaisen konesalin kaatumisen jälkeen.

Työn tuloksena Site Recovery Manager todettiin täysin toimivaksi peilausratkaisuksi konesalin kattavalta katastrofilta varautumisessa. Kriittisiä palveluja toissijaiseen konesaliin jatkuvasti varmistamalla ne voidaan nostaa korvaamaan kaatuneen ympäristön toimintaa tarpeen vaatiessa, ja näin vältytään suuremmilta palvelukatkoilta tai datan menetyksiltä.

ABSTRACT

Author(s): Toni Hietala

Title of the Publication: Securing Services with Datacenter Mirroring

Degree Title: Bachelor of Business Administration, Information Technology

Keywords: Mirroring, disaster recovery, Site Recovery Manager, replication

The objective of this thesis was to implement and test a solution for data center mirroring using VMware's Site Recovery Manager software. Data centers are often suspect to different threats that can damage their operation or even bring them down, thus causing significant financial loss if preparations have not been made.

The thesis was commissioned by Kajaani University of Applied Sciences and its practical part was executed in school's information system laboratory. The work covered the installation and testing phase of the environment as well as the theory underlying the subject.

Data center environments were virtualized on top of ESXi -hypervisors. VCenter Server was used to manage and vSphere Replication to enable replication on both virtual environments, both programs being appliance installations. Tests were completed successfully and services recovered to full function within an hour after the crash of the primary datacenter.

As a result of this work Site Recovery Manager was found to be a fully functional solution when preparing for a data center wide catastrophe with data center mirroring. By continuously backing up critical services to a secondary datacenter, the services can be brought back up when needed and thus greater service downtime and data loss can be avoided.

SISÄLLYS

1 JOHDANTO 1

2 KONESALIYMPÄRISTÖ 3
2.1 Rakenne 3
2.2 Virtualisointi 4

3 DISASTER RECOVERY 5
3.1 Riskianalyysi 5
3.2 Palautusstrategia 6
3.3 Palautussuunnitelma 6
3.4 Varmistus 7
3.5 Vikasietoisuus 8
3.6 Replikointi 8
3.7 Testaus 10

4 OHJELMISTORATKAISUT 11
4.1 Site Recovery Manager 11
4.2 AppAssure 12
4.3 Avamar 13
4.4 RecoverPoint 14
4.5 Veeam Availability Suite 15

5 CASE KAMK 17
5.1 Testiympäristön rakenne 17
5.2 Testiympäristön asennus ja konfigurointi 18
5.3 Testaus 30
5.4 Yhteenveto 33

6 POHDINTA 35

LÄHTEET 37

SYMBOLILUETTELO

Active Directory	Hallitsee verkkoympäristön muodostavien jaettujen resurssien, kuten tietokoneiden ja käyttäjien identiteettejä ja suhteita.
Appliance	Valmiiksi räätälöity ja tiettyä tarkoitusta varten paketoitu ohjelmisto, joka asennetaan sellaisenaan virtuaaliympäristöön.
Datastore	Levyjärjestelmä, datan sijaintipaikka.
Deduplikointi	Tiedon pakkaustapa, jolla eliminoidaan tarpeetonta dataa ja parannetaan varastoinnin hyötykäyttöä.
Disaster Recovery	Toimet ja menettelytavat, joilla konesali palautetaan toimintaan katastrofin jälkeen.
DNS	Nimipalvelujärjestelmä, joka auttaa verkon laitteita keskustelemaan keskenään.
Downtime	Aika jona järjestelmän palvelu ei ole saatavilla.
Fail-back	Toimintojen palauttaminen pääsijaiseen järjestelmään fail-over-toiminnon jälkeen.
Fail-over	Järjestelmän toimintojen käyttöönotto toissijaisessa järjestelmässä, kun pääsijainen ei ole saatavilla.
Fibre-Channel Fabric	Fibre Channel -laitteiden verkko, jossa verkon laitteet yhdistyvät usean kytkimen avulla.
Hypervisor	Virtuaalikoneita luova ja ajava hallintaohjelma, joka mahdollistaa usean käyttöjärjestelmän jakaa saman palvelimen resursseja.
IP-pool	Verkon asetus, jossa vCenter Server automaattisesti antaa IP-asetuksia virtuaalikoneille.

Isäntäkone	Virtualisointipalvelin, joka toimii alustana virtuaalikoneille.
Massamuistiohjain	Tallennuslaitteen ja tietokoneen välillä toimiva, tiedon ja komentojen vaihdon mahdollistava ohjain.
Migraatio	Datan siirtämistä järjestelmästä toiseen.
Replikointi	Datan jakamista resurssien välillä luotettavuuden, vikasietoisuuden tai esteettömyyden parantamiseksi
Resurssivaranto	Kokoelma laitteita ja niiden asetuksia, jotka asettavat rajat niillä ajettaville virtuaalikoneille.
RPO	Recovery Point Objective. Pisin mahdollinen aika, jolloin data saa olla menetettynä.
RTO	Recovery Time Objective. Tavoiteaika, jolloin yrityksen jokin toiminto täytyy olla palautettuna, jotta ei-hyväksyttäviltä vahingoilta vältyttäisiin.
Single-Sign-On	Keskitetty, useisiin palveluihin vain kerran kirjautumisen vaativa palvelu.
Tilatiedon kaappaus	Snapshot. Järjestelmän tilasta tiettynä ajankohtana otettu varmistus.
VCenter Server	Hallintatyökalu, jonka avulla voidaan hallita useita isäntäpalvelimia ja niiden virtuaalikoneita.
Virtuaalikone	Ohjelma, joka emuloi fyysistä tietokonetta.
Virtualisointi	IT resurssien teknisten piirteiden piilottaminen resursseja käyttäviltä järjestelmiltä, sovelluksilta ja loppukäyttäjiltä.

1 JOHDANTO

IT-järjestelmien tullessa entistä kriittisemmiksi organisaatioiden toiminnan kannalta on niiden varmistaminen toiminnan jatkumisen ja nopean palauttaminen valossa entistä tärkeämpää. Konesalin kaatuminen voi vakavuutensa takia ajaa yrityksen ahdinkoon, jollei hyvin suunniteltua toipumisratkaisua ole otettu käyttöön. Tällaisen tilanteen ennaltaehkäisy vaatii mahdollisten uhkakuvien tunnistamista ja datan suojausjärjestelmien perustamista. Häiriöistä selviytymisen ja downtimen minimoiminen on mahdollista vain varautumalla kaikenlaisiin onnettomuuksiin.

Varmin tapa varmistua ympäristön säilymisestä on perustaa toinen samankaltainen ympäristö erilleen itse konesalista. Toissijaisen konesalin sijainti pitäisi päättää siten, etteivät molemmat altistu samoille uhkatekijöille. Pääsijaisesta ympäristöstä pyritään siirtämään erilliseen ympäristöön palvelukriittisiä toimintoja niiden jatkuvuuden takaamiseksi. Tämä jatkuva varmistus eli peilaus on IT-palvelujen toiminnan kannalta oleellinen osa hyvää tietoturvaa.

Konesalin turvaamiseen on myös muita menetelmiä. Pilvipalveluna toteutettavan konesalin suojaamisen avulla kriittiset palvelut saadaan jonkin palveluntarjoajan kuten Amazonin ympäristön suojiin. Tällaiset suuret pilviympäristöt ovat maantieteellisesti hajautettuja, ja niiden tietoturva on myös niiden kokoluokan mukainen. Myös itse pääsijaisen konesalin suunnittelulla voidaan ehkäistä sen palveluihin kohdistuvia riskejä. Niin rakenteellisilla ominaisuuksilla kuin myös sijainnilla on suuri merkitys konesalin palvelujen turvaamisessa. Turvallisuus mielessä rakennettu, vahvarakenteinen ja valvottu konesali on askel parempaan konesaliturvallisuuteen. Myös itse konesalin sisäisen tietoturvallisuuden pitää olla kunnossa, jotta inhimillisiltä uhkilta, kuten viruksilta ja tietoturvahyökkäyksiltä vältyttäisiin mahdollisimman hyvin ja palvelujen turvallisuus saadaan taattua.

Tämän opinnäytetyön tarkoitus on keskittyä konesalin peilauksen mahdollistavaan Site Recovery Manager -ohjelmistoon ja sen taustalla olevaan teoriaan. Teoriaosuudessa keskitytään käsittelemään aihekokonaisuuksia konesaliympäristö, disaster recovery, vikasietoisuus ja replikointi sekä näihin kuuluvia käsitteitä, kuten palautussuunnitelmaa ja varmistusta. Lisäksi opinnäytetyössä käsitellään neljää

muuta vastaavanlaista varmistusohjelmistoa, joiden ominaisuuksia esitellään. Itse työn keskiössä oleva Site Recovery Manager -ohjelmisto on toimeksiantajan eli Kajaanin ammattikorkeakoulun valitsema. Ohjelmiston asennus toteutetaan Data-center-laboratorioon, jossa sen toiminnollisuutta ja ominaisuuksia testataan.

Työn tavoitteena on perehtyä konesalin peilaukseen ja pystyttää testiympäristö toimeksiantajan valitsemaa Site Recovery Manageria varten. Ympäristössä on tarkoitus toteuttaa virtuaalikoneiden palautusten ajamista kahden simuloidun konesalin välillä. Tavoitteena on, että työn tuloksena saadaan valmiudet samankaltaisen peilausjärjestelmän toteuttamiseen tuotantoympäristössä helposti toistettavan dokumentaation muodossa.

2 KONESALIYMPÄRISTÖ

Konesali on yrityksen osasto, jossa sen tarjoamien palveluiden vaatimat palvelimet ja tietovarastot sijaitsevat. Konesaleissa sijaitsevat organisaatioiden kriittisimmät järjestelmät päivittäisten toimintojen kannalta. Tästä syystä myös niiden turvallisuus ja luotettavuus ovat organisaatioiden suurimpia prioriteetteja. (Palo Alto Networks, 2015.)

Konesali voidaan yleisesti ottaen jakaa internet- ja yrityskonesaleihin. Ulospäin, internetiin suuntautuneet konesalit ovat yleensä selainpohjaisia, sovellusmääriltään suppeita ja käyttäjämäärältään suuria. Tällaisia konesaleja on esimerkiksi Facebookilla ja Amazonilla. Yritystarkoitukseen rakennettu konesali on yleensä pienemmälle käyttäjäkannalle tarkoitettu, monipuolisemmalla sovellusvalikoimalla varustettu kokonaisuus. (Palo Alto Networks, 2015.)

2.1 Rakenne

Konesali kokonaisuutena voidaan jakaa neljään osaan: tilat, tuki-infrastruktuuri, IT-laitteisto ja toiminnot. Konesali voi olla käytettävältä niin sanotulta korotetulta lattiapinta-alaltaan muutaman kymmenen tai jopa sadan tuhannen neliömetrin kokonaisuus. Tuki-infrastruktuuri kattaa kaiken lisälaitteiston ja tilan, jota konesali tarvitsee toimintojensa tueksi. Näitä ovat muun muassa varavirtalähteet (UPS), generaattorit ja ilmanvaihtojärjestelmät, jotka varmistavat konesalin katkottoman toiminnan. (CIO, 2009.)

IT-laitteiston osalta konesalin keskiössä ovat palvelimet, jotka mahdollistavat erilaisten palveluiden toiminnan, kuten verkkopalveluiden tarjoamisen asiakkaille tai tietokantojen ylläpidon. IT-laitteisiin kuuluvat myös kaapelointi, kehikot, tallennusjärjestelmät, hallintajärjestelmät ja erilaiset verkkolaitteet, kuten kytkimet, jotka mahdollistavat laitteiden kommunikoinnin keskenään ja palvelun käytön verkon yli. Toiminnosta vastaavan henkilökunnan tehtävä on varmistaa jatkuvalla valvonnalla IT-laitteiston ja infrastruktuurin oikeanlainen toiminta, käyttö, huolto, päivitys ja mahdolliset korjaukset. (CIO, 2009.)

2.2 Virtualisointi

Nykyaikaisessa konesaliympäristössä suuri osa palvelinlaitteistosta on virtualisoitu tilojen, virran ja jäähdytyksen kustannusten vähentämiseksi. Virtualisoinnin ansiosta yritykset voivat vähentää tarvittavan laitteiston määrää, koska resursseja voidaan allokoida tarpeen mukaan aina sinne missä niitä tarvitaan. Tämä edesauttaa myös lämmöntuoton hallinnassa, sillä mitä vähemmän lämpöä tuottavia palvelimia on, niin sitä vähemmän kustannuksia konesalin jäähdytyksessä tarvitaan. (Wallen, 2013.)

Virtualisoinnista on myös apua hallinnallisissa toimissa, kuten käyttöönotoissa tai varmistusten tekemisessä. Virtuaalisessa ympäristössä kokonaisen virtuaalipalvelimen varmistuksen lisäksi myös virtuaalikoneista voidaan ottaa varmistuksia ja tilatiedon kaappauksia. Virtuaalikoneita voidaan halutessa siirtää palvelimelta toiselle ja ottaa käyttöön nopeasti ja helposti. (Wallen, 2013.)

Konesalien energiankulutus on yksi IT-alan merkittävimpiä haasteita niiden jatkuvasti suurenevan kulutuksen vuoksi. Tässä yhtenä merkittävänä apukeinona on virtualisointi, joka edesauttaa taloudellisten säästöjen lisäksi myös yritysten vihreiden arvojen omaksumista IT:n suhteen. Virtualisointi yhdessä korkean tiheyden blade -palvelimien ja tietovarastojen kanssa on edesauttanut palvelinten tarvitseman energiamäärän vähentämisessä. (Wallen, 2013.)

3 DISASTER RECOVERY

IT-henkilöstön työ organisaatiossa on tietojärjestelmien saatavuuden varmistamista niin arkisessa työelämässä kuin myös katastrofin sattuessa. Disaster Recovery eli katastrofista palautuminen on prosessi, joka varmistaa organisaation toiminnan jatkuvuuden katastrofin sattuessa. Riskejä tarkastellaan isossa mittakaavassa ja valmistaudutaan koko konesalia koskeviin vaaratilanteisiin, toisin kuin vikasietoisuuden tai testauksen suhteen, jolloin mittakaava on järjestelmäkohtainen. Prosessissa keskitytään keskeisten toimintojen palautusten lisäksi myös palautusprosessin toteuttamiseen mahdollisimman lyhyessä ajassa. Mahdollisimman täydellisen palautuksen saavuttamiseksi lyhimmässä mahdollisessa ajassa luodaan suunnitelma, jota kutsutaan palautussuunnitelmaksi (disaster recovery plan). (Varghese, 2002.)

3.1 Riskianalyysi

Mahdolliset organisaation konesaliin ja siten yritystoiminnan palveluihin kohdistuvat katastrofitason riskit voidaan jakaa luonnonkatastrofeihin ja ihmisten aiheuttamiin katastrofeihin. Luonnonkatastrofeihin lukeutuvat muun muassa maanjäristykset, myrskyt ja tulvat. Ihmisen aiheuttamia ovat muun muassa tulipalot, varkaudet, vandalismi ja sabotaasi. (Iivari & Laaksonen, 2009.)

Riskianalyysi on keskeinen osa toipumissuunnitelman laadintaa. Todennäköisimmät ja vakavimmat uhkatekijät voidaan tunnistaa hyvällä toipumissuunnitelmalla. Osa näistä on mahdollista minimoida kokonaan ja toisiin varautua riskin pienentämisellä tai siirtämisellä. Riskianalyysissä jää usein huomioimatta riskejä, joihin ei voida suoranaisesti varautua tai joita ei ole edes tunnistettu mahdollisiksi riskeiksi. (Iivari & Laaksonen, 2009.)

3.2 Palautusstrategia

Onnettomuus, jossa konesalin virtuaali- ja isäntäpalvelimet ajautuvat alas, voi sattua, vaikka kuinka varmistettaisiin palvelinten ja niiden palveluiden turvallisuus. Tästä syystä on erittäin tärkeää valmistautua vikatilanteita varten. Mitä enemmän dataa suojaavia menetelmiä käytetään järjestelmissä, sitä todennäköisempää on mahdollisen downtimen minimoiminen ja datan säilyminen. Yrityksen täytyy koosta riippumatta turvautua standardiin järjestelmänpalautusstrategiaan laitteiston suojelemiseksi. Palautusstrategia on siis organisaation yleisen tason suunnitelma ongelmatilanteisiin varautumisessa. (Ruest & Ruest, 2009.)

Palautusstrategia kattaa kokonaisuudessaan riskien lieventämisen, kohtuuhintaisuuden pitkällä aikavälillä ja testauksen. Lieventääkseen riskejä täytyy organisaation varmistaa järjestelmien vikasietoisuus ja datan suojeleminen häiriötilanteessa. Hyvässä palautustrategiassa data on varastoituna myös toiseen paikkaan kuin päätoiminen konesali ja kaikesta ainakin kopiot esimerkiksi nauhalle tallennettuna. Yleisimmät datan varastointivaihtoehdot ovat nauha ja levy. Lisäksi myös pilvipalvelu on varteenotettava vaihtoehto perinteisten varastointimuotojen rinnalla. Sen käyttöönottoa ovat hidastaneet toistaiseksi kohtuuttomat kustannukset ja huoli tiedon turvallisuudesta. (Spectra, 2011.)

3.3 Palautussuunnitelma

Palautussuunnitelma on dokumentoitu, yksityiskohtainen etenemissuunnitelma IT-järjestelmien palauttamiseksi toimintaan, kun katastrofi on iskenyt. Itse prosessi, jonka tuloksena suunnitelma saadaan aikaiseksi, on katastrofista palautumisen suunnittelu (disaster recovery planning). Suunnittelun toteuttamisella taataan nopea ja kustannustehokas toimintojen palautus ja jatkuvuus, katastofista riippumatta. (Varghese, 2002.)

Vaikkei täysin jokaista riskiä varten ole dokumentoitu palautussuunnitelmaa, niin ainakin palvelukriittisimpiä tilanteita varten sellainen on oltava tehtynä, jotta yritys-

toiminnan jatkuvuus voidaan taata esimerkiksi mahdollisen tulvan varalta. Kun ensin mahdollinen ongelma taikka palvelun keskeytys havaitaan, selvitetään, onko se virtuaalikone- vai resurssivarantokohtainen. Kyseinen ongelma täytyy sitten tutkia ja kategorisoida esimerkiksi standardin vianetsintästrategian mukaan, jonka jälkeen siihen liittyvää riskiä arvioidaan sen mukaan, kuinka kiireellisiä toimia se vaatii. Esimerkiksi itse isäntäpalvelin vaatii toimintakriittisyytensä takia korkeamman prioriteetin kuin sen alla toimiva virtuaalikone. Kun vikatilanne on saatu tunnistettua, niin sen mukaisiin palautussuunnitelman toimenpiteisiin voidaan ryhtyä. Kun palautussuunnitelman mukainen palautustoimenpide on tehty, kannattaa suorittaa testaus, jotta kaiken voidaan varmistaa toimivan oikein. Tapauksen jälkeen se tulisi dokumentoida ja tarpeen mukaan palautussuunnitelmaan liittyvät etenemisprosessit päivittää. (Ruest & Ruest, 2009.)

3.4 Varmistus

Data on yksi tärkeimmistä varmistettavista asioista konesaleissa. Tähän lukeutuvat organisaation dokumentit kuin myös fyysiset palvelimet ja virtuaaliset palvelimet. Vaikka palvelimet pystytäänkin asentamaan uudelleen, vie asennus aikaa ja vaivaa. Palvelujen varmistuksen avulla mahdollisilta hukkaan menevältä työtunneilta voidaan välttyä. Varmistuskäytännöstä päätettäessä tulee miettiä, kuinka usein ja millaisia varmistuksia halutaan ottaa. Myös tallennusmedia, esimerkiksi levyjärjestelmä tai nauha, tulee päättää. (Varghese, 2002.)

Varmistusten kierrosta täytyy päättää, eli kuinka usein vanhat varmistukset korvataan uusilla. Varmistuskäytänteeseen vaikuttaa, kuinka paljon resursseja organisaatiolla on käytössään. Otettujen varmistusten palautus tulee myös testata, jotta tiedetään, onko varmistusympäristöstä mitään hyötyä. Myös otettujen varmistusmedioiden oikeaoppinen ylläpito ja eheyden tarkistus täytyy muistaa tehdä. (Varghese, 2002.)

3.5 Vikasietoisuus

Järjestelmän vikasietoisuus perustuu menetelmiin ja toimenpiteisiin, jotka täytäntöön pantuna varmistavat, että komponentin rikkoutuessa sen toiminnollisuus automaattisesti korvataan toisen komponentin toimesta. Vaikka tällaista automaatiota ei pystyttäisikään toteuttamaan, on toiminnon palautus vähintään oltava ylläpitäjien tuntema ja hyvin dokumentoitu. Jotta järjestelmä olisi täysin vikasietoinen, täytyy resurssivarannon jokaisen elementin olla suojattu. Näitä ovat muun muassa datan varastointitila, palvelimet, hallintatietokannat ja hallinnasta vastaavat virtuaalikoneet. (Ruest & Ruest, 2009.)

Onnettomuuksilta varautumisessa paras keino on toissijainen konesali, jolloin tärkeimmät palvelimet ja palvelut ovat saatavilla useammassa kuin yhdessä paikassa. Sen ei tarvitse olla täysin samanlainen kokoonpanoltaan, vaan riittää, että se kykenee ylläpitämään tarvittavia palveluja sen aikaa, kunnes pääsijainen konesaliympäristö saadaan takaisin pystyyn. Toinen konesali ottaa toiminnan haltuun päätoimisen lamaantuessa, jolloin vältytään suuremmalta palvelukatkolta. Palvelukriittistä dataa sisältävien resurssivarantojen jatkuvuus taataan replikointiteknologioiden avulla, jotka replikoivat dataa konesalista toiseen. (Ruest & Ruest, 2009.)

3.6 Replikointi

Replikointi on merkittävä osa kriittisen tiedon turvaamista palvelinympäristöissä ja yksi keskeinen tekijä Disaster recovery -ohjelmissa. Replikointi voidaan jakaa ominaisuuksiltaan neljään eri kategoriaan: tallennusjärjestelmäpohjaiseen (array-based), isäntäpohjaiseen (host-based), hypervisor-pohjaiseen ja verkkopohjaiseen replikointiin.

Tallennusjärjestelmäpohjainen

Tallennusjärjestelmäpohjaisessa replikoinnissa keskenään yhteensopivat tallennusjärjestelmät käyttävät sisäänrakennettuja ohjelmistoja automaattiseen datan kopioimiseen tallennusjärjestelmien välillä. Kyseiset replikaatio-ohjelmat toimivat

massamuistiohjaimilla, jotka sijaitsevat levytallennusjärjestelmissä. (Rouse, 2012a.)

Isäntäpohjainen

Isäntäpohjaisessa replikoinnissa käytetään palvelimia datan kopioimiseen paikasta toiseen. Replikointi tapahtuu sovelluspalvelimella sijaitsevan ohjelmiston toimesta, joka lähettää datan muutoksia toiselle laitteelle. Tämä prosessi on yleensä asynkroninen ja tiedostopohjainen. Tehokkuuden ja turvallisuuden takaamiseksi ohjelmistot käyttävät erilaisia menetelmiä datan kopioimisessa, kuten salausta deduplikointia ja dataliikenteen pakkausta. (Rouse, 2012b.)

Hypervisor-pohjainen

Hypervisor-pohjainen replikointi on hyvin lähellä isäntäpohjaista replikointia, suurimpana erona hieman korkeampi toimintataso, eli replikointi tapahtuu hypervisortasolla resurssitason sijaan. Hypervisor-pohjaisessa replikoinnissa virtuaalikovalevyjen tai kokonaisien virtuaalikoneiden kopioita luodaan ja ylläpidetään automaattisesti. Perinteisiä varmuuskopioita ei luoda, koska replikointi on jatkuva taustalla toimiva prosessi. (Posey, 2012.)

Synkronisesti ylläpidetyt kopiot eivät sovellu esimerkiksi kansio-, tiedosto- tai sovellusten palautukseen, koska replikoitava kopio on yleensä sisällöltään täysin peilattu versio alkuperäisestä. Esimerkiksi jos tiedosto poistetaan pääsijaiselta virtuaalikoneelta, poistuu se myös sen kopiolta. (Posey, 2012.)

Verkkopohjainen

Verkkopohjaisessa replikoinnissa käytetään hallintalaitetta, joka sijaitsee paikallisverkossa isäntäpalvelinten ja tallennusjärjestelmien välissä. Se jakaa I/O:t joko itse verkkolaitteessa tai Fibre Channel fabricissa. Läpi kulkevan I/O:n kuuluvuus replikointivolyymiin tarkastetaan, ja jos se sellaiseen kuuluu, niin sen kopio ohjataan määritettyyn replikointikohteeseen. (Gsoedl, 2011.)

3.7 Testaus

Vikasietoisuustestauksen tulisi olla keskeinen osa jokaisen organisaation katastrofipalautus-, tietosuoja- ja yritystoiminnan jatkuvuuden prosesseja. Se on tärkeä osa tietoturvaa, joka tulee usein laiminlyödyksi. Vikasietoisuutta arvioivat testit voivat paljastaa virheitä suunnitelmissa, prosesseissa, arkkitehtuurissa, päätöksissä, olettamuksissa ja tuotteissa. Asiantunteva IT-henkilö ennakoi ja korjaa mahdolliset viat testauksen avulla, eliminoiden tai ainakin minimoiden liiketoimintaa haittaavat riskit. (Staimer, 2014.)

Resurssit, aika, henkilöstö ja budjetti määrittävät, kuinka usein testausta voidaan toteuttaa. Liiketoiminnan jatkuvuuden parhaiden käytäntöjen mukaan vikasietoisuuden testaus tulisi suorittaa aina neljännesvuosittain. Ensimmäinen vaihe vikasietoisuustestauksen toteutuksessa on hallinnon sitoutuminen testauksen määräaikaiseen ja säännölliseen suorittamiseen. (Staimer, 2014.)

Tämän jälkeen tulisi tehdä datan ja sovellusten arviointi, jossa arvot määräytyvät RPO:n ja RTO:n perusteella. Seuraava vaihe on datan ja sovellusten priorisointi, eli mitkä sovellukset ja niiden data täytyy olla ensimmäisinä saatavilla. Myös kaikki työntekijöiden toimintaohjeet täytyy selvittää ongelmatonta testausta varten. (Staimer, 2014.)

Kun kaikista vikasietoisuustestauksen prosesseista ja menettelytavoista on päätetty, lopuksi voidaan laatia kirjallinen suunnitelma. Siitä käy ilmi vaadittavat toimenpiteet, päävastuuhenkilö, hänen varahenkilö ja odotetut aikataulut toimenpidekohtaisesti. Tiivistettynä testauksessa on kyse valmistelusta, priorisoinnista, harjoittelusta ja kärsivällisyydestä. (Staimer, 2014.)

4 OHJELMISTORATKAISUT

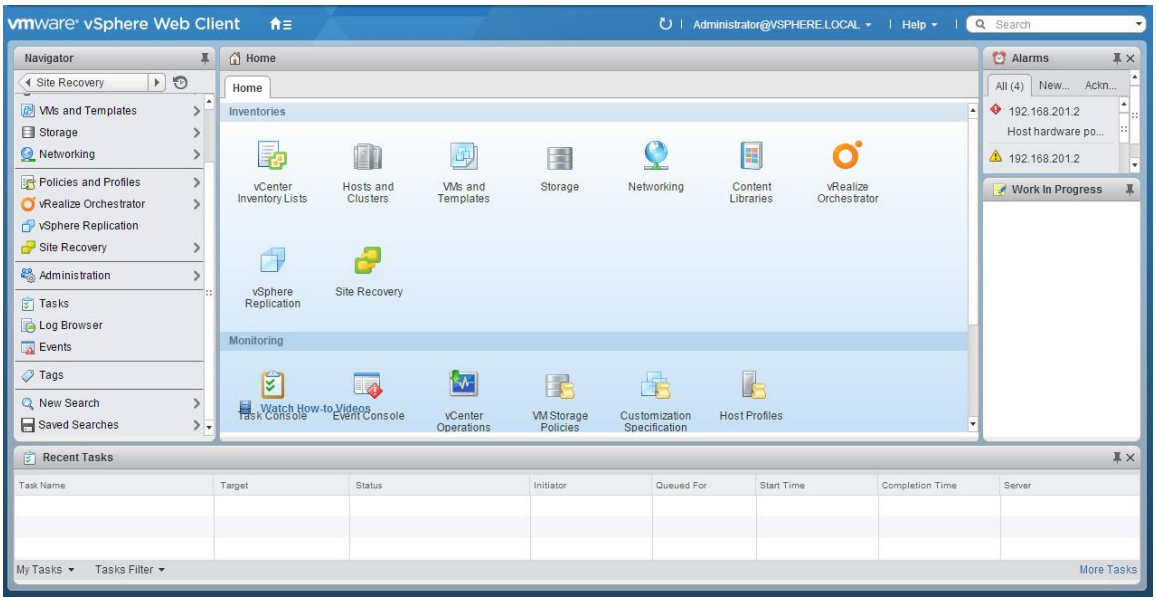
Tässä osiossa esitellään katastrofista palautumisen ja replikoinnin toteuttamisessa käytettäviä ohjelmistoja. VMwaren vCenter Site Recovery Manager -ohjelmisto valittiin työhön toimeksiantajan pyynnöstä, ja siksi se on näistä ainoa, joka tullaan käytännössä toteuttamaan testiympäristöön. DELLin AppAssure, EMC:n Avamar ja RecoverPoint sekä Veeam valittiin esittelyyn niiden samankaltaisen tarkoitusperän vuoksi, joka on katastrofista palautumisen toteuttaminen varmistusten ja replikoinnin avulla.

4.1 Site Recovery Manager

VMware vCenter Site Recovery Manager on disaster recovery ja liiketoiminnan jatkuvuuden ohjelmaratkaisu. Tämä VMwaren kehittämä, vCenterin toimiakseen vaativa katastrofista palautumisen ohjelma auttaa suunnittelemaan, testaamaan ja ajamaan virtuaalikoneiden palautumisia pääsijaisen ja toissijaisen konesalin välillä. Site Recovery Manager -ohjelmaa käytetään vSphere Web Clientin kautta kuvan 1 mukaisesti. (VMware, 2015a.)

Replikointiin voidaan käyttää isäntäpohjaista vSphere Replication -ohjelmaa, jolloin kyseinen Site Recovery Managerin ulkopuolinen, vCenter ympäristön liitännäisohjelma vastaa virtuaalikoneiden työkuormien suojaamisesta. Replikointiin voidaan käyttää myös tallennusjärjestelmäpohjaista replikointia, jolloin levyjärjestelmien välillä replikoidut tietokannat palautetaan virtuaalikoneiden työkuormien turvaamiseksi. (VMware 2015b.) Näistä ratkaisuista vSphere Replication on suositeltavin toteuttaa yksinkertaisemman ja yhteensopivamman käytön vuoksi. Tallennusjärjestelmäpohjaisessa ratkaisussa tarvitaan myös tallennusjärjestelmien replikointiadapterit, jotta replikointi toimisi. (VMware 2015c.)

Site Recovery Managerilla toteutettavat palautussuunnitelmat voivat olla aina yksittäisiä virtuaalikoneita tai kokonaisia konesaleja koskevia. Konesalien välillä on mahdollista palauttaa haluamiaan kokonaisuuksia edestakaisin ja testata katastrofista palautumista omien tarpeiden ja aikataulujen mukaan. (VMware 2015c.)



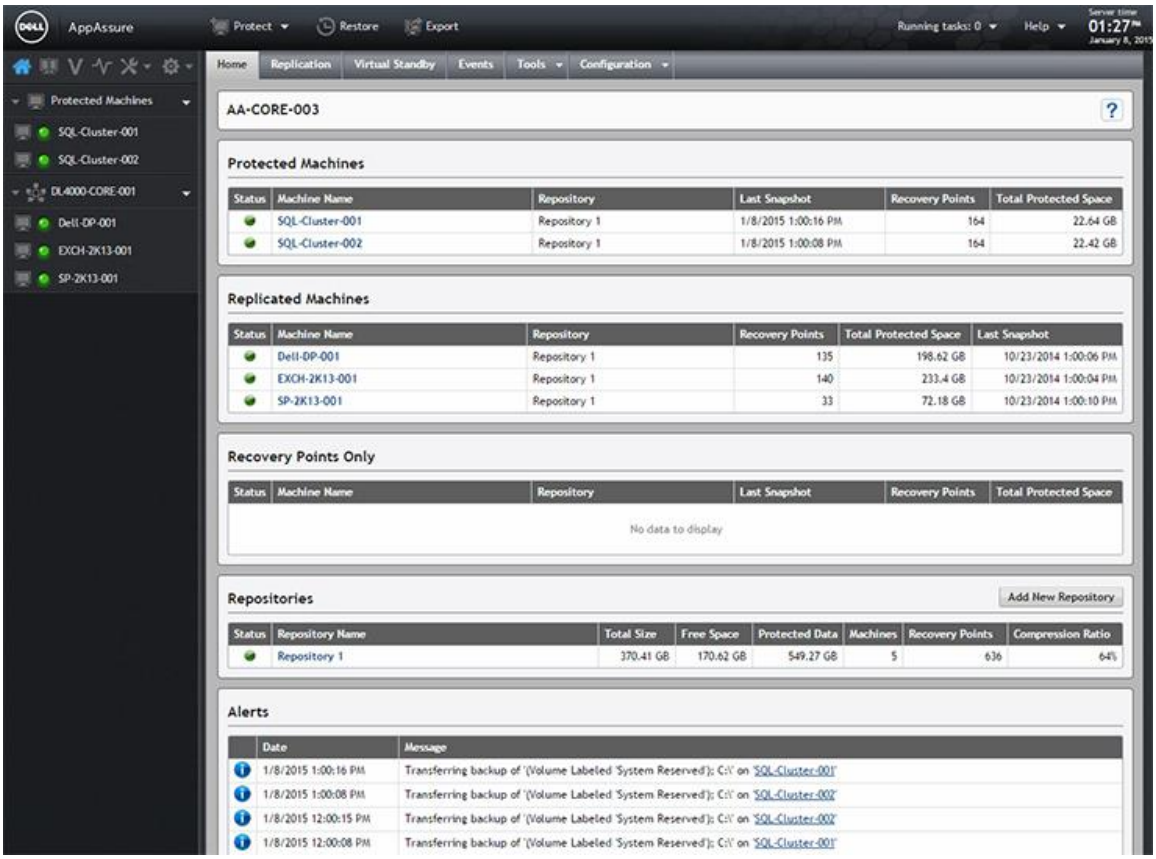
Kuva 1. Kuvaruutukaappaus Site Recovery Manager -ohjelmasta.

4.2 AppAssure

AppAssure on DELLin ohjelmistoratkaisu varmistusten, replikoinnin ja palautusten hoitoon. Replikoinnissa, toisin kuin Site Recovery Manager, AppAssure käyttää omaa sisäänrakennettua isäntäpohjaista replikointimoottoria. (DELL, 2014a.)

Replikointiympäristö koostuu AppAssure Core -palvelimista ja suojattavilla koneilla sijaitsevista agenteista. AppAssure tarjoaa kahdenlaista replikointistrategiaa: multi-hop, jossa suojattu agentti replikoidaan yhtä aikaa lukuisille Core-palvelimille, ja chained replication, jossa replikointi tapahtuu ketjumaisesti ensin yhdelle Core-palvelimelle ja joka replikoi sen taas seuraavalle. (DELL, 2014b.)

Katastrofin sattuessa AppAssure mahdollistaa palvelimen ohjelman ja tietojen saatavuuden palvelukatkoksesta huolimatta varmuuskopion avulla. Lisäksi myös fyysisen koneen dataa voidaan siirtää virtuaalikoneelle, luoden helposti saatavan, käynnistettävän kopion koneen ohjelmista ja datasta. AppAssuren vaatimuksena kuitenkin on, että käsiteltävät koneet ovat Windows-käyttöjärjestelmällä varustettuja. AppAssure käyttää integroitua deduplikointia ja tiedostojen pakkausta varastointitilan säästämiseksi. AppAssuren käyttöliittymä voidaan nähdä kuvasta 2. (DELL, 2014a.)

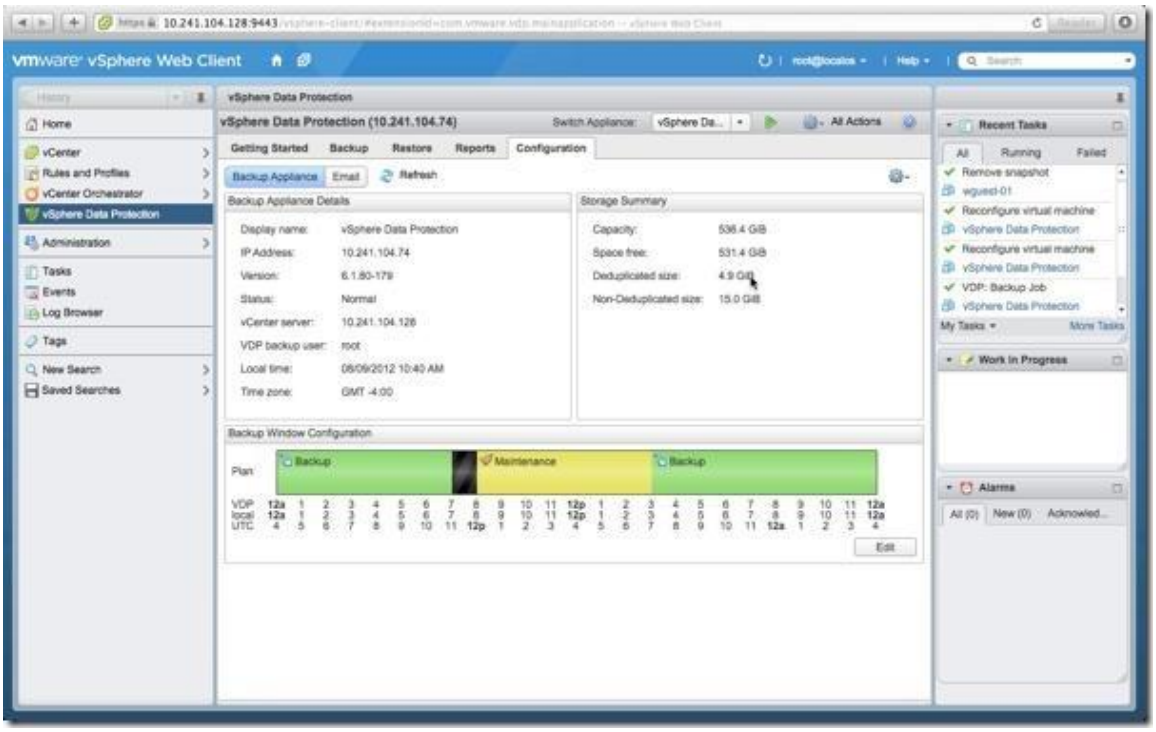


Kuva 2. Kuvaruutukaappaus AppAssure-ohjelmasta. (DELL, 2014c.)

4.3 Avamar

Avamar on EMC:n tarjoama ratkaisu varmistusten ja palautusten hoitoon. Se käyttää AppAssuren tavoin deduplikointia välttyäkseen tarpeettomalta datalta jo clientin päässä, ennen varmistettavan datan lähettämistä verkon yli. Samalla myös verkon kuormitus vähenee jopa 99 prosenttia. Varmistusdatan deduplikointia tapahtuu myös konesalitasolla palvelimia myöten, jolloin säästetään levyjärjestelmäkapasiteettia. Avamar tarjoaa myös oman replikointiratkaisunsa katastrofista palautumiseen. (Avamar, 2014.)

Avamarin teknologia toimii useiden ohjelmien, kuten VMwaren Data Protectionin alla. Se tarjoaa agentitonta, levykuva -tason virtuaalikoneiden varmistusta vSphere-ympäristössä kuvan 3 mukaisesti. (VMware, 2015d.)



Kuva 3. Kuvaruutukaappaus Avamar-pohjaisesta ohjelmasta. (Seagrave, 2012.)

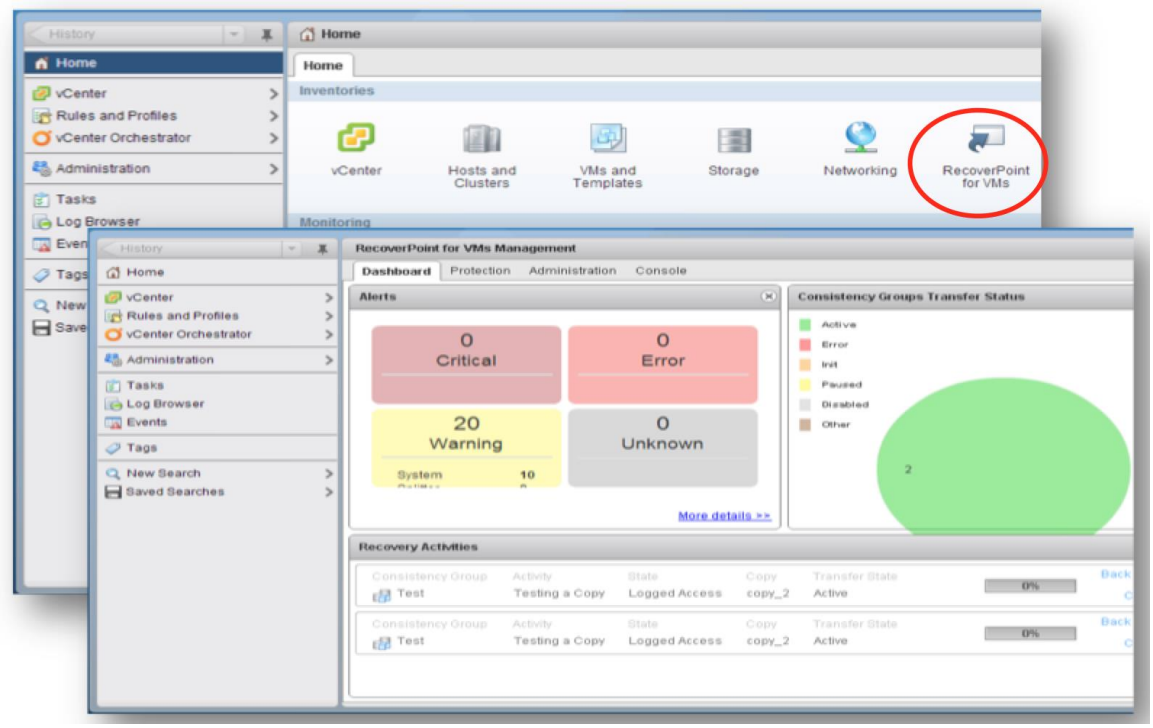
4.4 RecoverPoint

RecoverPoint on EMC:n tarjoama replikointiratkaisu, joka pyrkii yksinkertaistamaan ja automatisoimaan organisaation tiedonsuojausta ja katastrofista palautumista. Nimensä mukaisesti se mahdollistaa palautuksen tekemisen haluttuun ajankohtaan. (EMC, 2014.)

RecoverPoint-tuoteperhe koostuu kahdesta tuotteesta: RecoverPoint for Virtual Machines ja RecoverPoint. Molemmat tuoteperheen jäsenet tarjoavat samankaltaisia ominaisuuksia jaetun arkkitehtuurinsa vuoksi. RecoverPoint for Virtual Machines mahdollistaa paikallisen ja etänä toteutettavan virtuaalikoneiden replikoinnin niin suojatun ja toissijaisen konesalin välillä kuin myös paikallisestikin. Se on VMware hypervisor -pohjainen, ohjelmistotason tiedonsuojaustyökalu, jota käytetään vCenter-ympäristön kautta lisäsovelluksena, kuten kuvan 4 kuvaruutukaappauksesta voidaan nähdä. (EMC, 2014.)

RecoverPoint keskittyy virtuaalikoneiden sijasta suoraan tallennusjärjestelmien suojaukseen ja integroituu EMC:n valmistamien tallennusjärjestelmien kanssa.

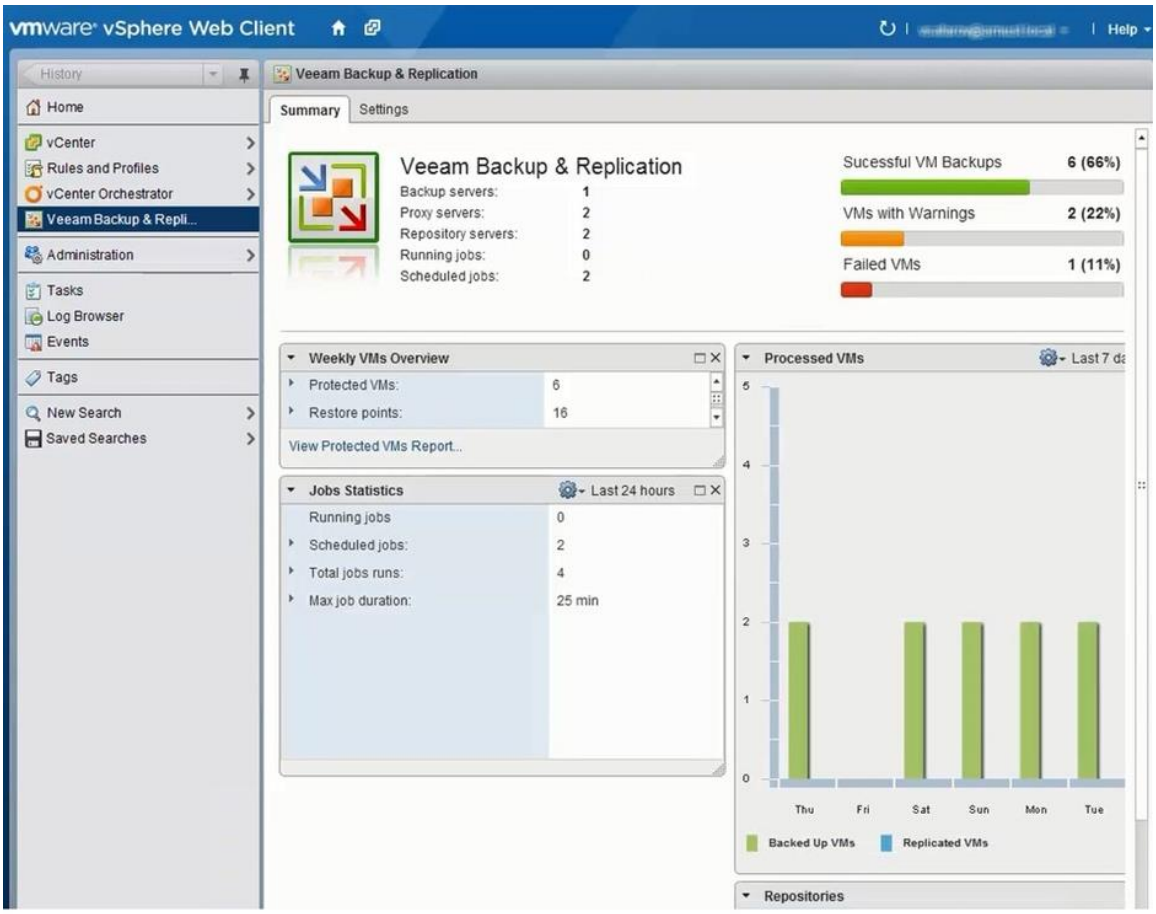
RecoverPoint voi toimia myös VMware Site Recovery Managerin kanssa, jolloin se toimii sen levyjärjestelmäpohjaisena replikointiratkaisuna, laajentaen suojausmahdollisuuksia pelkkään kuvakaappaukseen verrattuna. (EMC, 2014.)



Kuva 4. Kuvaruutukaappaus RecoverPoint-ohjelmasta. (Fritsch, 2014.)

4.5 Veeam Availability Suite

Veeam Availability on Veeamin tarjoama tuotekokonaisuus, jonka Veeam Backup & Replication -osa mahdollistaa varmistusten, palautusten ja replikoinnin toteutuksen. Availability Suiten Veeam ONE -ohjelma tarjoaa mahdollisuuden IT-ympäristön monitorointiin, raportointiin ja suunnitteluun. Availability Suite soveltuu niin VMware vSphere kuin myös Microsoft Hyper-V -ympäristöjen turvaamiseen ja hallintaan. Tuotetta voidaan käyttää joko oman hallintakonsolinsa tai vSphere Web Clientin kautta, kuten kuvasta 5 voidaan nähdä. (Veeam, 2015.)



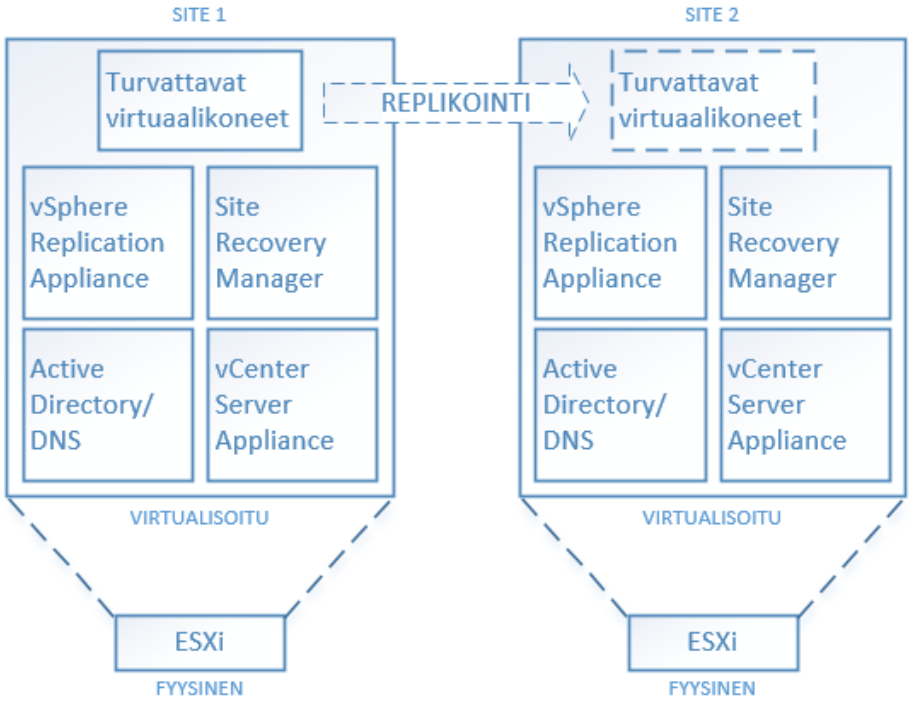
Kuva 5. Kuvaruutukaappaus Veeam Backup & Replication -ohjelmasta. (Veeam, 2013.)

5 CASE KAMK

Opinnäytetyön käytännön työ tehtiin Kajaanin ammattikorkeakoulun tietojärjestelmälaboratoriossa kesällä 2015. Tavoitteena oli pystyttää ja testata VMwaren vCenter Site Recovery Manager -ohjelmiston katastrofista palautumisen ominaisuuksia tietojärjestelmälaboratorion tiloihin pystytetyssä ympäristössä. Replikointitavaksi valittiin vSphere Replication -ohjelman käyttö.

5.1 Testiympäristön rakenne

Fyysinen ympäristö koostuu kahdesta PowerEdge R410 -palvelimesta, joille on asennettu ESXi 5.5. Ympäristö on datacenter-laboratorion konesalissa. Palvelimet muodostavat kukin toiminnaltaan oman konesalin, jotka pyörittävät omia virtualisoituja vCenter Server Appliance 6.0-, Active Directory-, DNS-, vSphere Replication 6.0- ja Site Recovery Manager 6.0 -palvelimia. Pääsijaisessa konesalissa sijaitsevat myös virtuaalikoneet, joita käytetään turvattavina kohteina. Ympäristön suunniteltu rakenne on esitetty kuvassa 6.



Kuva 6. Testiympäristön rakennesuunnitelma.

5.2 Testiympäristön asennus ja konfigurointi

Tässä luvussa käydään läpi vaiheet ja toimet, joita testiympäristön pystytyksen aikana tehtiin. Käsittelyssä on jokainen ympäristön rakenneosa, kuten fyysiset palvelimet, hypervisorit ja virtualisoidut palvelimet. Lisäksi tässä luvussa perehdytään myös tarpeen mukaan jokaisen rakenneosan kohdalla tehtyihin asetuksiin. Työssä käytettiin olemassa olevia palvelimia, jotka olivat jo valmiina asennettuna tietojärjestelmälaboratorion palvelinkaappiin.

Site Recovery Manager -ympäristö vaatii, että molemmissa konesaleissa on DNS-palvelu, vSphere host ja Microsoft Windows -virtuaalikone, jossa vCenter Site Recovery Manager asennettuna. Lisäksi konesaliympäristöissä täytyy olla joko tallennusjärjestelmäpohjainen replikointi tai vSphere Replication käyttöönotettuna ja säädettynä sekä Windows- tai Linux-pohjaisia virtuaalikoneita, joissa on VMware Tools asennettuna ja joita suojataan Site Recovery Managerin avulla. (VMware, 2015c.)

ESXi

Palvelimille asennettiin ESXi 5.5 -versio muistitikkua käyttäen. Kyseinen versio on yhteensopiva suunnitellun 6.0-ympäristön kanssa. Asennuksessa täytyi määrittää asennuskohde, näppäimistökieli ja root-käyttäjän salasana. Kyseinen asennusprosessi sujui ongelmitta.

Asennuksen jälkeen ESXi:llä täytyi määrittää sen IP-asetukset, jotta sitä voitaisiin hallita vSphere-ympäristöstä käsin. Asetuksista täytyi muistaa tarkistaa, että oikea verkkokortti oli valittuna ja että palvelimille varatut staattiset IP-asetukset tulivat niiden asettamisen jälkeen voimaan. Molempien palvelimien IP-asetuksissa määritettiin myös DNS ja Hostname sekä suoritettiin pienimuotoinen verkkoyhteyksien testaus Network test -kohdassa, jossa ping-komennolla kutsuttiin verkon laitteita. Kutsut onnistuivat, joten siirryttiin seuraavaan asennusosioon.

DNS/AD

Palvelinten muodostamille ympäristöille tehtiin omat DNS- ja Active Directory Domain Controller -palvelimet. Asennus aloitettiin ottamalla ESXi -ympäristöihin verkon yli yhteys vSphere Clientilla. Asennusmediaksi valittiin Windows 2012 R2 Enterprise, jonka asennuksessa määritettiin muun muassa tuoteavain ja Administrator salasana. Käyttöliittymäksi valittiin Graafinen vaihtoehto Core-version sijaan.

Asennuksen jälkeen virtuaalikoneelle asetettiin sille varattu staattinen IP ja vaihdettiin koneen nimi helpommin ymmärrettäväksi ja sen toimintaa kuvaavaksi. Pääsijaisessa konesalissa eli Site 1:n kohdalla nimeksi asetettiin Site1AD ja toissijaisen Site 2:n kohdalla vastaavasti Site2AD. Nimenvaihdon jälkeen palvelin täytyy käynnistää uudelleen. Tämän jälkeen tehdään itse Active Directory- ja DNS-roolien asennus Server Manager -ikkunan Add roles and features -valikosta. Asennuksen jälkeen voidaan asettaa DNS:lle forward- ja reverse lookup zone -asetukset. Jokaista ympäristön virtuaalikonetta vastaavat IP-asetukset täytyy löytyä asetetuista arvoista, tai muuten IP-pohjaiset nimikyselyt eivät toimi. Tätä tarvitaan erityisesti vCenter appliancen tapauksessa, sillä jos asetusta ei ole tehty, ilmoittaa se asennusvaiheessa virheestä. Testiympäristössä pystytettyjen domainien nimiksi valittiin pääsijaisessa konesalissa thor ja toissijaisessa konesalissa loki.

VCenter Server Appliance

Konesaliympäristöissä täytyy olla vSphere ja vSphere Web Client -asennukset käyttöönotettuna. Testiympäristössä tämä toteutettiin Windows Server 2012 R2 -pohjaiselle virtuaalikoneelle, jolle myös Site Recovery Manager aiotaan asentaa.

vCenter 6.0:n asennus toteutettiin HTML-setup-menetelmää käyttäen, ensin asennusmedia ISO -imagen lataamalla jollekin konesaliympäristön virtuaalikoneelle, tässä tapauksessa Site Recovery Manageria varten pystytetylle virtuaalikoneelle. Ensiksi asennetaan median vcsa-kansiosta löytyvä Client Integration Plug-in ja sitten juuresta löytyvä vcsa-setup.html-tiedosto, joka käynnistää appliancen asennusprosessin. Asennus on lähes OVF-template-käyttöönoton kaltainen, eli appliance asennetaan virtuaalikoneeksi ympäristön muiden koneiden joukkoon, mutta nyt asennus hoidetaankin jonkin virtuaalikoneen sisältä käsin eikä suoraan vSphere-ympäristöstä.

VMware vCenter Server Appliance:n käyttöönoton aikana määritetään ensin kohde ESXi-isäntäpalvelin ja luotavan virtuaalikoneen asetukset nimineen ja salasanoineen. VCenterin käyttöönoton aikana täytyy valita sisäisen ja ulkoisen Platform Service Controllerin välillä. Kyseinen palvelu hallitsee muun muassa Single Sign-On-, lisenssi- ja sertifikaattipalveluja. Tässä työssä valittiin sisäinen vaihtoehto, koska silloin ei tarvita erillistä virtuaalikonetta hallitsemaan kyseistä palvelua ja koska testiympäristö on vain yhden vCenter-palvelimen kokoinen molemmissa konesaleissa.

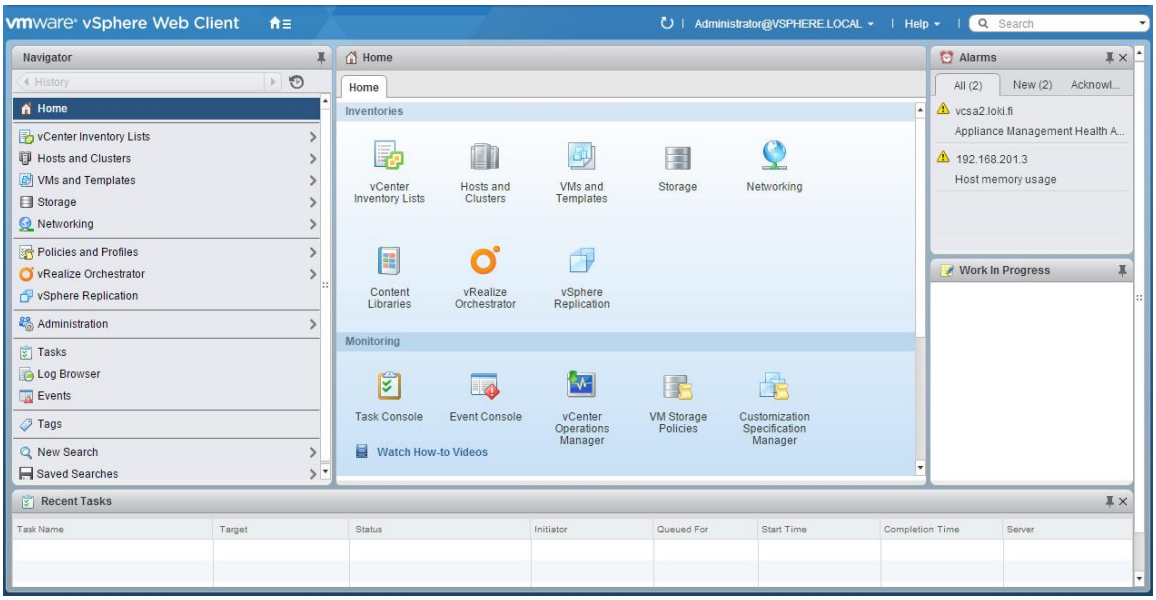
SSO Domain -kohdassa luodaan vCenter-ympäristöön kirjautumiskäytäntö, eli millä nimellä ja salasanoilla minkä nimiseen ympäristöön tullaan jatkossa kirjautumaan. Appliancen kooksi valittiin Tiny, koska ympäristö tulee olemaan vain alle kymmenen virtuaalikoneen kokoinen. Asennuksen aikana on mahdollista valita, käyttääkö vCenterin sisäistä tietokantaa, joka on vPostgres, vaiko Oraclen tietokantaa. Näistä sisäinen on suositeltavin vaihtoehto, ja se valittiin tätä testiympäristöä pystytettäessä. IP-asetusten jälkeen appliance on valmis asennukseen, jonka jälkeen siihen voidaan ottaa yhteys vSphere web clientillä. VCenter liitetään lopuksi vielä domainiin Administration-valikosta.

VSphere Replication

Jos Site Recovery Manager asennetaan ennen vSphere Replication Appliancea, ilmenee ympäristössä ongelmia. Asennusvaiheessa Site Recovery Manager tarkistaa vSphere Replicationin olemassaolon, ja jos sitä ei silloin ole, niin ei se myöskään tule jälkikäteen asennettuna toimimaan. Asennettavana mediana toimii ISO:sta löytyvä tavallinen OVF10-asennus eikä AddOn-niminen versio, jota käytettäisiin lisäreplikointitarpeessa.

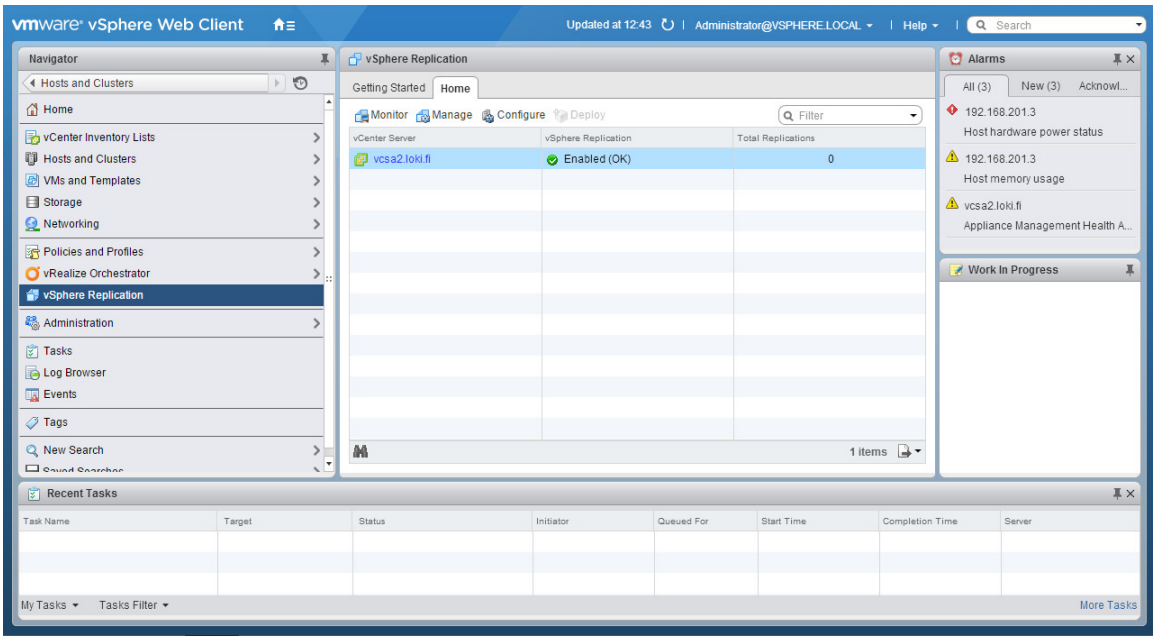
Asennusvaiheessa määritetään tavallisten isäntäpalvelimen sijainnin ja datastoren lisäksi myös IP asetukset, jotka valitaan DHCP-, staattinen- tai Transient-IP-vaihtoehtojen välillä. Työssä käytettiin Transient-IP-asetuksia, jolloin tarvitaan myös ennen appliancen asennusta valmiiksi asetettu IP-pool, josta appliance ottaa IP:nsä käyttöön. Asennuksessa määritetään myös replikoinnin kannalta kriittiset NTP-palvelimet, joiden avulla konesalien replikointi ajastetaan yhtenäiseksi. Testiympäristössä NTP-palvelimiksi valittiin julkiset 0.fi.pool.ntp.org-palvelimet,

jotka lisättiin peräkkäin, vain pilkulla erotettuna asennuksen NTP-palkkiin. Asennettaessa vSphere Replication Appliance liittyy sille osoitettuun vCenter-palvelimeen liitännäiseksi. Kun Appliance on käyttöönotettu vSphere-ympäristössä, täytyy ensin kirjautua ulos ja takaisin ennen kuin sen asennus voidaan havaita kuvan 7 mukaisesti vSpheren Inventory-osiossa.



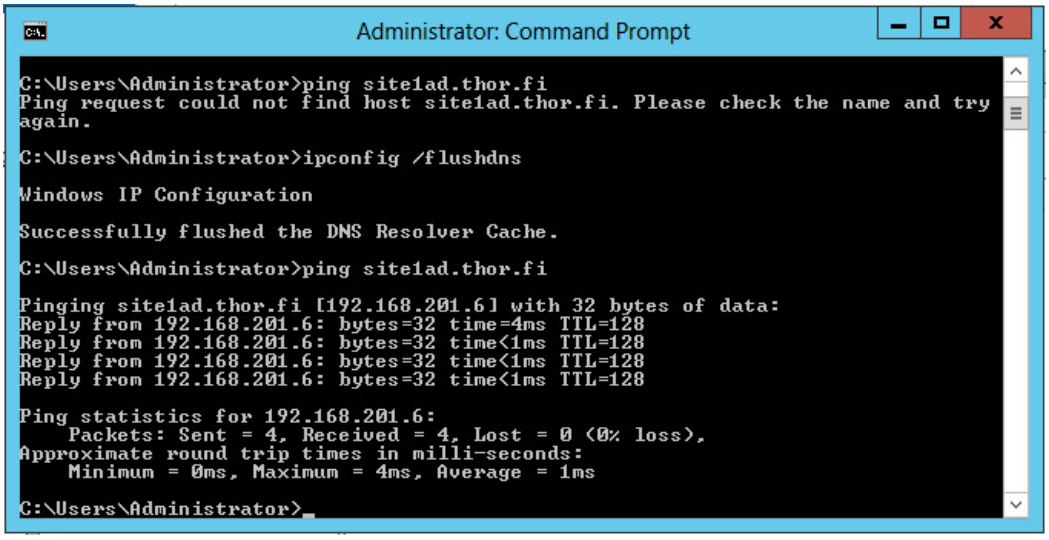
Kuva 7. Kuvaruutukaappaus vSphere Replication -ohjelmasta vSphere-ympäristössä.

Käyttöönoton jälkeen siirrytään vielä vSphere Replicationin VAMI-näkymään rekisteröintiä varten osoitteessa https://appliance-osoite:5480. Sisään kirjautumisen jälkeen mennään Configruation-välilehteen ja varmistetaan, että Lookup Service Address on määritettunä vCenter-palvelimen FQDN-osoitteeseen. Lisäksi Networking-välilehdeltä asetetaan Appliancen nimi ja domain omaan ympäristöön sopiviksi. Kun asetukset ovat kunnossa, valitaan Save and Restart Service -painike rekisteröinnin ja palvelun käynnistämisen suorittamiseksi. Lisäksi hyväksytään SSL sertifikaatti -huomautus, joka ilmestyy pian kyseisen toiminnon aloittamisen jälkeen. Rekisteröinnin jälkeen napsauttamalla vSphere Replication -kuvaketta Web Clientissä päästään tarkastelemaan sen tilaa, joka tulisi näyttää Enabled (OK) kuvan 8 mukaisesti.



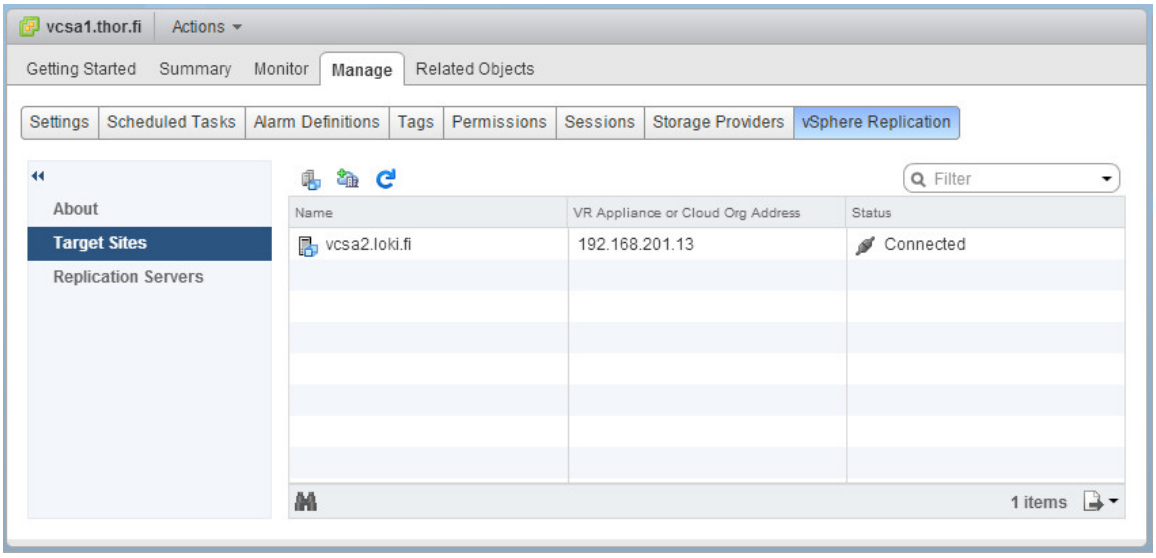
Kuva 8. Kuvaruutukaappaus vSphere Replicationin tilasta.

Kun asennus ja rekisteröinti on molemmissa konesaleissa tehty, voidaan siirtyä replikointiyhteyksien määrittämiseen. Menemällä vSphere Replication -osioon ja Manage-välilehdelle voidaan valita Target Sites kohdasta Connect to target site -ikonia. Kohteen määrittämisessä käytetään täyttä FQDN-nimeä, jonka toimimiseen täytyy olla molemmissa konesaleissa DNS-palvelimen forwarder ja Conditional forwarder määritettynä osoittamaan toisen ympäristön DNS-palvelimeen. Tämän jälkeen myös DNS täytyy resetoida ipconfig /flushdns -komennolla kuvan 9 mukaisesti, jotta asetukset alkavat toimimaan.



Kuva 9. Kuvaruutukaappaus DNS-palvelimen /flushdns-operaatiosta.

Tämä mahdollistaa FQDN-kyselyt domainien välillä, ja virheilmoituksilta säästytään kohteen määrityksen aikana. Onnistuneen yhdistämisen tuloksena Target Sites -kohdasta voidaan nähdä yhteys Connected-tilassa kuvan 10 mukaisesti. Myös kohteena olevassa vSphere-ympäristössä voidaan havaita yhdistetyn vCenterin ilmoitus.



Kuva 10. Kuvaruutukaappaus vSphere Replicationin yhteydestä.

Testikoneet

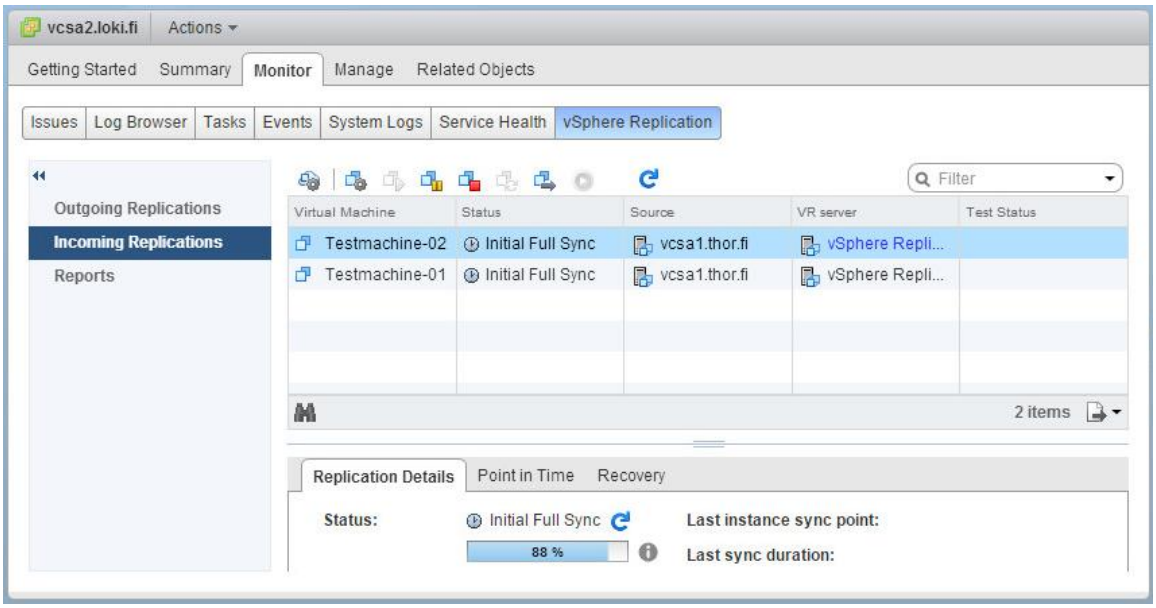
VSphere Replicationia ja Site Recovery Manageria varten pystytetään kaksi Windows Server 2012 R2 -virtuaalikonetta. Näillä Testmachine-01- ja Testmachine-02-nimisillä koneilla, jotka eivät ole muun testiympäristön kannalta kriittisiä, testataan replikoinnin ja palautussuunnitelman toimivuutta. Kyseisille virtuaalikoneille täytyy määrittää replikointi ennen seuraavia vaiheita.

Oikealla hiiren napilla valitsemalla haluttu virtuaalikone ja menemällä All vSphere Replication Actions -kohtaan saadaan näkyviin Configure Replications, jossa replikointiasetukset voidaan määrittää. Määrityksissä tulee vastaan Target site -osio, jossa valitaan replikoinnin kohdesijainti. Tässä on mahdollista valita replikointi suoritettavaksi joko paikalliseen tai ulkoiseen ympäristöön. Tässä testiympäristössä valittiin ulkoinen kohde, joka Site 1 -ympäristön kannalta oli Site 2:n palvelin vcsa2.loki.fi. Replication options -osiossa on mahdollista määrittää replikoinnin kannalta erilaisia ominaisuuksia, kuten Enable network compression for VR data,

joka helpottaa verkon kuormaa ja muistin käyttöä mutta kasvattaa vastaavasti prosessorin kuormitusta. Kyseinen vaihtoehto vaatisi saman ESXi- ja vCenter-version ollakseen toteutettavissa, joten sitä ei testiympäristössä voitu edes valita, koska käytössä oli ESXi 5.5 ja vCenter 6.0.

Recovery Settings -osiossa määritetään virtuaalikoneen Recovery Point Objective (RPO) ja Point in time instances. RPO:n avulla voidaan määrittää kyseisen virtuaalikoneen datahävikin sietokyky, eli kuinka pitkältä ajalta dataa voidaan hyväksyttävästi menettää, jos konesalin toiminnassa tapahtuu jokin häiriö. Replikointi suoritetaan siis joka kuudes tunti, jos RPO on kuusi tuntia. Mitä pienempi kyseinen arvo on, sitä useammin virtuaalikone replikoidaan ja sitä enemmän prosessi vie ympäristön resursseja. Testiympäristössä RPO:ksi valittiin 6 tuntia. Point in time instances -määrityksen avulla voidaan valita, halutaanko virtuaalikoneen replikoiduista istunnoista tehdä kuvakaappauksia ja kuinka monta minkäkin ajan verran tallessa. Kyseistä ominaisuutta ei valittu testiympäristössä käytettäväksi.

Kun replikointi on asetettu virtuaalikoneelle, käynnistyy replikointi konesalien välillä. Tämä alustava replikointi kestää pidempään kuin sitä seuraavat, vain muutoksia replikoivat kerrat. Prosessia voidaan tarkastella vSphere Replication -osion Monitor-kohdasta. Riippuen siitä, onko kyseessä pääsijainen eli replikointidataa lähettävä, vai toissijainen eli replikointidataa vastaanottava konesali, ilmenee replikointitapahtuma eri paikoissa. Kuvassa 11 on vastaanottavan ympäristön eli Site 2:n näkymä alustavasta replikoinnista, kun molemmille testikoneille on määritetty replikointi.



Kuva 11. Kuvaruutukaappaus alustavasta replikoinnista.

Site Recovery Manager

Site Recovery Managerin asennuksessa määritetään Platform Services Controller, joka tämän testiympäristön tapauksessa on samalla palvelimella kuin itse vCenter. Kyseinen asennus suoritettiin aiemmin mainitulle Windows Server 2012 R2 -virtuaalikoneelle. Asennuksen aikana määritetään myös paikallisen isäntäkoneen osoite ja käytettäviä sertifikaatteja koskevat määritteet. Myös Site Recovery Managerin Sites-osiossa näkyvä nimi määritetään siten, että se on helposti tunnistettavissa. Testiympäristössä käytettiin nimiä Site 1 ja Site 2.

Lisäksi valitaan joko sisäinen tai ulkoinen tietokanta, joka tässä testiympäristössä valittiin sisäiseksi ympäristön pienen koon vuoksi. Asennus toistetaan myös toisen konesalin kohdalla, vastaavine asetuksineen. Asennuksen loputtua Site Recovery Manager ilmestyy vSphere Web Client -ympäristöön.

Lopuksi Site Recovery Manager -istunnot täytyy vielä liittää toisiinsa. Tämä tapahtuu menemällä Sites-valikon Objects-välilehdelle ja valitsemalla Pair Site -ikoni. Määritettävä on vain Platform Services Controller, joka on toisen Site Recovery Manager -ympäristön vCenterin FQDN-osoite. Kyseinen asetus vaatii kohteen SSO -tunnuksia rekisteröinnin suorittamiseksi. Kun toisen konesaliympäristön istunnon kanssa ollaan tekemisissä Site Recovery Manager -ympäristössä, kysyy se tunnuksia yhteyden muodostukseen. Tämä voidaan hoitaa myös menemällä

jommankumman ympäristön Sites -osioon ja valitsemalla Login Site sekä syöttämällä tarvittavat tunnukset.

Konesalien parituksen jälkeen voidaan huomata, että Sites-osiosta jompikumpi saleista valittaessa löytyy sivun alhaalta Guide to configuring SRM -ikkuna kuvan 12 mukaisesti. Onnistuneen käyttöönoton saavuttamiseksi on suositeltavaa seurata kyseisen ohjeen ehdottamaa järjestystä. Ainoa sivuutettava vaihe on osio 4, koska testiympäristössä käytetään tallennusjärjestelmäpohjaisen replikoinnin sijaan isäntäpohjaista vSphere Replikointia. Tämän luvun seuraavat osat etenevät ohjeen mukaisesti.

Kuva 12. Kuvaruutukaappaus Site Recovery Managerin määrittämisohjeesta.

Inventory mappings

Inventory mappings -määrittämisen avulla voidaan vaikuttaa siihen, miten Site Recovery Manager kartoittaa virtuaalikoneiden resursseja. Protection Group jakaa tämän kartoituksen kaikille virtuaalikoneilleen. Kartoituksessa määritellään tärkeimmät virtuaalikoneita koskevat ominaisuudet, kuten verkot, kansiot, laitteistoresurssit ja placeholder datastoret. Lisäksi suoritetaan Prepare reverse mappings, joka luo vastaavat kartoitukset paritettuun konesaliin. Ilman näitä määrityksiä Site Recovery Manager ei voi suojata virtuaalikoneita. Vaihtoehtoja ovat resurssi, kansio- ja verkkopohjainen kartoitus. Testiympäristössä tehtiin resurssikartoitus-vaihtoehto.

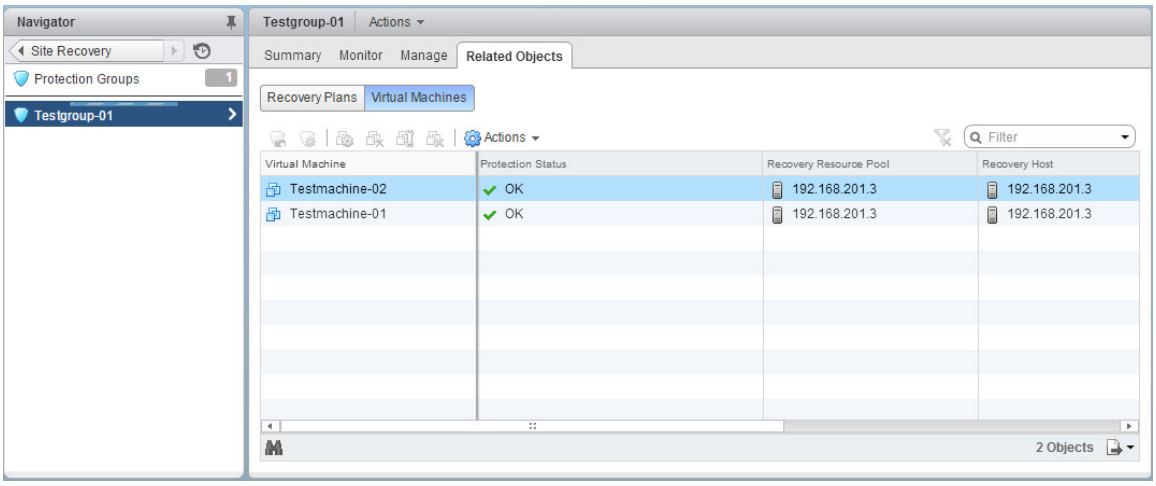
Placeholder datastore

Placeholder datastore on sijainti, johon jokaista protection groupin virtuaalikonetta varten luodaan tilapäinen versio kustakin virtuaalikoneesta toissijaiseen konesaliin. Itse placeholder datastoren määrittämisessä valitaan vain haluttu datastore kohteeksi. VSphere Replicationia käytettäessä tämä datastore ei saisi olla sama kuin replikoinnin kohteena oleva datastore, jolloin on mahdollista törmätä ongelmiin palautussuunnitelman reprotect-toiminnon yhteydessä. Tämä tehdään vielä toisessakin konesalissa.

Protection group

Protection groupin avulla määritetään suojeltavien virtuaalikoneiden ryhmä. Vain virtuaalikoneet, joille on määritetty replikointi, voidaan liittää tällaisiin ryhmiin. Create protection group -toiminnon aikana määritetään sen nimen lisäksi, joka testiympäristössä oli Testgroup-01, myös suojattava konesali. Tässä ympäristössä Site 1 valittiin tuohon Protected Site -rooliin. Lisäksi valittiin itse suojattavat virtuaalikoneet, joita oli luotu ja replikoitu valmiiksi kaksi kappaletta.

Määrityksen jälkeen kannattaa varmistaa protection groupin tila menemällä Site Recovery Managerin Protected Groups -osioon kuvan 13 mukaisesti ja tarkistaa virtuaalikoneiden suojauksen tila. Jos Protection Status on jotain muuta kuin OK, niin yksittäistä virtuaalikonetta voi säätää sen suojausasetusten osalta. Testiympäristön kohdalla Testgroup-01:n tila ei ollut OK, koska virtuaalikoneisiin oli jäänyt levy liitetyksi, joka piti irrottaa vikailmoituksen korjaamiseksi. Onnistuneen protection groupin luonnin jälkeen suojatut virtuaalikoneet ilmestyvät omanlaisine ikoneineen recovery-konesalin vSphere-näkymään.



Kuva 13. Kuvaruutukaappaus Protection Groupin virtuaalikoneiden tilasta.

Palautussuunnitelma

Palautussuunnitelman avulla määritetään, miten Site Recovery Manager suorittaa virtuaalikoneiden palautuksia. Create a recovery plan -toiminnon avulla päästään määrittämään recovery-konesali ja kyseiseen palautussuunnitelmaan halutut protection groupit. Lisäksi täytyy valita, millaisia verkon asetuksia halutaan käyttää testejä ajettaessa. Oletuksena oleva Auto-vaihtoehto luo testivaiheessa tilapäisen ja eristetyn testiverkon, eikä näin häiritse muun ympäristön toimintaa. Testiympäristön palautussuunnitelmassa käytettiin verkon oletus-asetusta ja suunnitelman nimeksi annettiin Testrecovery. Palautussuunnitelman valmistuttua se ilmestyy Site Recoveryn Recovery Plans -välilehdelle ja on näin valmis testattavaksi. Testaukseen perehdytään seuraavassa luvussa.

Huomioitavaa asennusprosessista

Ympäristön pystytys ei mennyt suunnitelmien mukaan, ja aikataulusta jäätiin jälkeen asennusten aikana ilmenneiden ongelmien vuoksi. Yksi asennusprosessin ongelmallisimpia vaiheita oli vSphere Replication- ja Site Recovery Manager -ohjelmien yhteensopivuuden toteuttaminen. Ympäristöä lähdettiin pystyttämään sillä oletuksella, että vSphere Replication asettuu toiminnallisesti Site Recovery -ohjelman päälle ja täytyy siis asentaa vasta tämän jälkeen. Useiden uudelleenasennusten jälkeen asia todettiin päinvastaiseksi ja työ sai jatkua seuraavaan ongelmaan saakka.

Seuraava ongelmakohta asennusvaiheessa liittyi vSphere Replication appliancen NTP-asetuksiin. vSphere Replicationin Home-osiossa oli pitkään Configuration error -virheilmoitus, joka ilmoitti, ettei NTP-asetuksia ole kyseiselle palvelimelle määritettynä, vaikka NTP -palvelin määritettiin asennusvaiheessa. Ongelmaa lähdettiin ensin ratkaisemaan luullen, että vika on vSphere Replication appliancen ulkopuolinen. Ratkaisua haettiin muun muassa määrittelemällä NTP-palvelin vCenter- ja DNS-palvelimille sekä lopettamalla vSphere Replication appliancen aikasynkronointi isäntäpalvelimen kanssa. Lopulta ongelmaksi paljastui uudelleenasennuksen yhteydessä NTP-asetuksen virheellinen määrittäminen välimerkeillä.

Konesalien vSphere-replikoinnin toisiinsa liittämisen yhteydessä ilmeni virheilmoitus, ettei liitettävänä olevan konesalin nimeä tai palvelua tiedetä. Tätä virheilmoitusta ratkottiin ensin varmistamalla, että kaikki testiympäristön virtuaalikoneet löytyvät DNS-palvelimen Reverse Lookup Zone -listasta. Kyseinen ratkaisu ei ainakaan yksinään auttanut, joten ratkaisua haettiin liittämällä DNS-palvelimet toisiinsa siten, että nimikyselyt ohjautuvat nimipalvelimelta toiselle forwarderin ja Conditional forwarderin avulla. Tämän jälkeen liittäminen onnistui, ja se voidaan nähdä asennusvaiheen vSphere Replication -osassa.

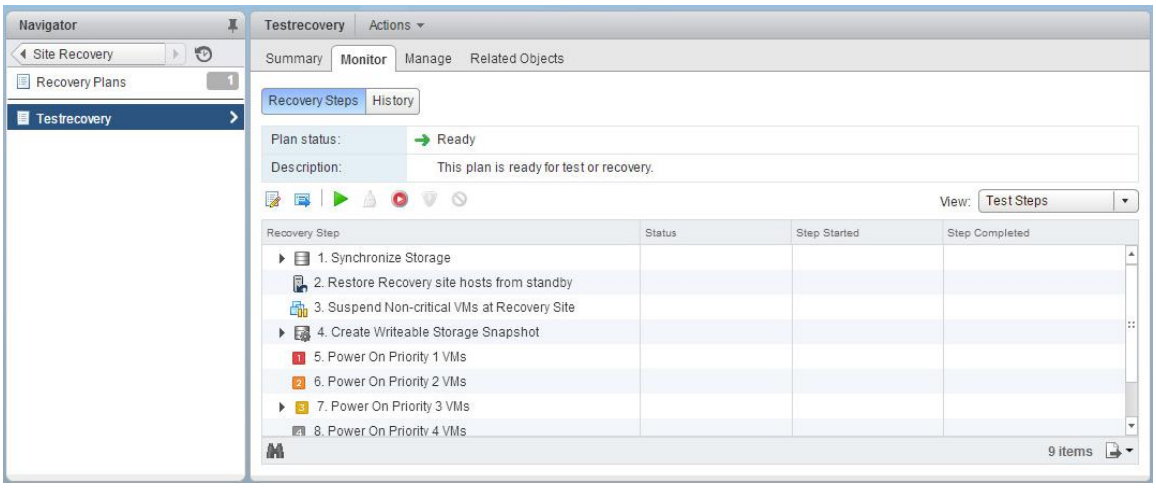
Konesalien nimeäminen koitui myös ongelmalliseksi. Tarkoituksena oli pitää yhtenäinen nimeämiskäytäntö läpi asennusvaiheen ja nimetä Site Recovery -näkymässä olevat konesalit Site 1- ja Site 2 -nimisiksi. Huomaamatta toisen nimi oli jäänyt oletukseksi eli tässä tapauksessa vcsa2.loki.fi-nimiseksi ja konesalit oli jo keretty parittaa keskenään. Sinänsä pienestä esteettisestä ongelmasta tuli suurempi, kun nimeä halusi muuttaa eikä se onnistunut ilman Site Recovery -ympäristöjen täydellistä uudelleenasennusta. Kun ympäristöt oli ehditty parittaa, oli niiden välille muodostettu nimisidonnainen datarakenne, jota toinen ympäristö ei yksin voi muuttaa. Esimerkiksi kun uudelleenasensi vain kyseisen Site Recovery Manager -ohjelman toisella nimellä, ei yhteyttä kyetty muodostamaan, koska sellainen oli jo toisen ympäristön mukaan olemassa.

5.3 Testaus

Tässä luvussa käydään läpi Site Recovery Manager -ympäristössä suoritetut testit sekä niihin liittyviä asetuksia. Testiympäristössä suoritettiin palautussuunnitelman ja fail-back-ominaisuuden testaus.

Palautussuunnitelman testaus

Jotta palautussuunnitelman toimivuus voidaan varmistaa, täytyy se ensin testata. Site Recovery Managerissa halutun palautussuunnitelman valitsemalla ja ajamalla sen testauksen painamalla Test recovery plan -painiketta päästään testin käynnistysikkunaan. Sen avulla määritetään, halutaanko aloitettavassa testissä replikoida viimeaikaisia muutoksia, jolloin replikointi suoritetaan vielä uudestaan palautussuunnitelman testiajoa varten. Itse testi etenee vaihe kerrallaan kuvan 14 mukaisesti.



Kuva 14. Kuvaruutukaappaus palautussuunnitelman testausnäkymästä.

Testin jälkeen voidaan tarkastella eri vaiheiden statusta ja niihin liittyviä ilmoituksia. Vaikka Plan status -kohdassa näkyisikin Test complete, ei se takaa palautussuunnitelman täyttä onnistumista. Tästä syystä täytyy tarkistaa, että kaikki vaiheet ovat Success-tilassa, jotta testi voidaan katsoa onnistuneeksi ja valmiiksi oikeaa palautusprosessia varten. Jos testissä kuitenkin ilmeni ongelmia, voi yksityiskohtaisen raportin tapahtuneesta nähdä siirtämällä hiiren kyseisen kohdan päälle.

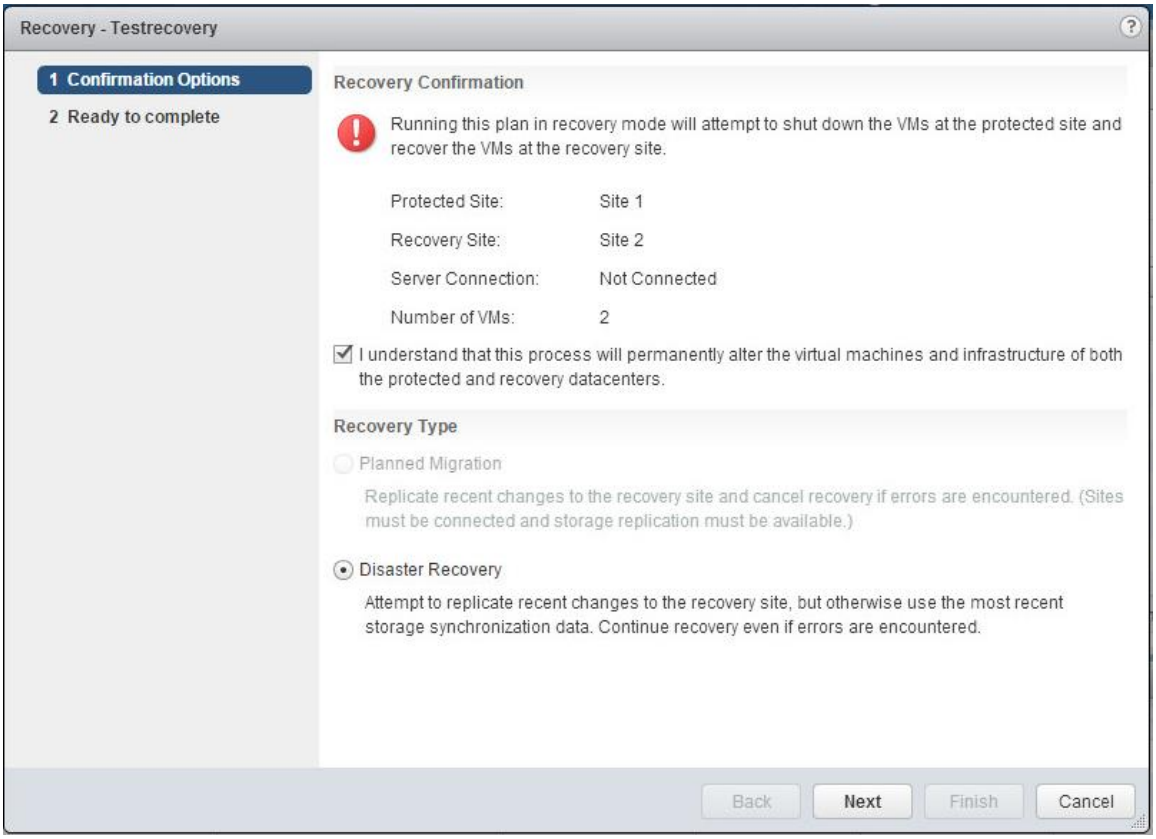
Onnistuneen testin jälkeen palautussuunnitelman sisältämiä virtuaalikoneita voi tarkastella recovery-konesalissa ja testata niiden toiminnollisuutta. Kun testaus todetaan valmiiksi, voidaan se puhdistaa Site Recovery Manager -ympäristöstä Cleanup recovery plan -toimintoa käyttäen. Kyseisen toiminnon aikana testiin liittyvät virtuaalikoneet sammutetaan ja niihin liittyvät kuvakaappaukset poistetaan. Puhdistusprosessin tuloksena palautussuunnitelmaa voidaan taas testata tai ajaa oikeasti.

Oikean palautussuunnitelman ajo hoituu Run recovery plan -toiminnon avulla. Sen valitsemalla avautuu määritysikkuna, jossa on vaihtoehtoina planned migration ja disaster recovery. Planned migration -vaihtoehdon kohdalla Site Recovery Manager olettaa, että kyseessä on suunniteltu, mahdollisesti ennakoiva palautustoiminto. Tämän avulla saadaan varmemmin viimeisin data siirrettyä uuteen ympäristöön pystytettäville virtuaalikoneille. Kyseinen vaihtoehto ei ole valittavissa, jos suojattava konesali on alhaalla esimerkiksi katastrofin takia. Tällöin ainoana vaihtoehtona on disaster recovery, jonka suorittamalla Site Recovery Manager palauttaa suojattavat virtuaalikoneet recovery-konesalissa toimintaan viimeisintä replikoitua dataa käyttäen.

Testiympäristössä palautussuunnitelma ajettiin molemmilla komennoilla, ensin planned migration -menetelmällä tarkkaillen molempien konesalien tapahtumia prosessin aikana. Suoritettuaan ensin replikoinnin ja sammutettuaan protected-konesalin virtuaalikoneet sekä varmistettuaan isäntäpalvelimien päällä olon valmistelee palautussuunnitelma virtuaalikoneet migraatiota varten. Migraation ja pystytyksen jälkeen suojatut virtuaalikoneet ovat toimintakunnossa recovery-konesalissa. Koska testiympäristön suojattavana kokonaisuutena oli vain kaksi virtuaalista palvelinkonetta, kesti itse palautussuunnitelman ajo vain noin tunnin.

Disaster recovery -ratkaisua varten testiympäristön Site 1 -ympäristö eli protected-roolin konesali ajettiin alas. Kuvan 15 mukaisesti määritysikkuna ei edes anna valita muuta vaihtoehtoa kuin disaster recovery, koska se tunnistaa ongelman konesalien välisessä yhteydessä. Määrityksen yhteydessä varmistetaan myös, että recovery-toimintoa suorittava on tietoinen konesaleissa tämän seurauksena tapahtuvista muutoksista. Prosessi on vaiheiltaan planned migration -toiminnon kanssa

lähes sama, mutta disaster recovery -toiminto ohittaa protected-konesalia koskevat vaiheet yhteysongelman takia. Tämä ilmenee virheilmoituksina kyseisten vaiheiden kohdalla. Molemmissa menetelmissä virtuaalikoneet liitetään myös protected-konesalin verkkoon.



Kuva 15. Kuvaruutukaappaus Disaster recovery -prosessin käynnistyksestä.

Reprotect ja Fail-back

Jos recovery-konesaliin siirretyt eli fail over -menetelmällä pystytetyt virtuaalikoneet halutaan palauttaa alkuperäiseen konesaliympäristöönsä, on suoritettava fail back. Tämä on mahdollista vain jos konesali on toimintokunnossa. Fail back -toimintoa ennen täytyy suorittaa reprotect recovery plan -työnkulku. Tämä voidaan käynnistää palautussuunnitelman Monitor-välilehdeltä. Tämän tuloksena palautussuunnitelma ja replikointi käännetään toimimaan vastakkaiseen suuntaan. Alkuperäinen protected-konesali siis vaihtuu recovery-konesaliksi ja alkuperäinen recovery-konesali protected-konesaliksi.

Jotta konesalien tila ja virtuaalikoneet halutaan niiden alkuperäisiin osoitteisiinsa, täytyy palautussuunnitelma ajaa reprotect-toiminnon jälkeen. Tämän tuloksena

virtuaalikoneet siirretään takaisin alkuperäiseen konesaliin ja nostetaan siellä toimintakuntoon. Viimeistelyksi pitää vielä ajaa reprotect-toiminto, jotta protection groupin määritykset vastaavat uusia protected- ja recovery-määrityksiä. Tämän operaation jälkeen Site Recovery Manager -ohjelman toiminto on onnistuneesti testattu ja disaster recovery -testiympäristö voidaan todeta toimivaksi.

Palautusasetusten kustomointi

Site Recovery Managerin avulla voidaan muokata sillä suoritettavien palautussuunnitelmien virtuaalikoneita muun muassa niiden IP-asetusten osalta. Tällöin niiden verkkoliitännät voidaan määrittää muuttuvaksi halutun laiseksi kun niille suoritetaan fail-over tai fail-back. Lisäksi virtuaalikoneiden virta -tiloja palautuksien sammutus- ja käynnistysvaiheissa voidaan muokata siten, että esimerkiksi ne jätetäänkin sammutetuiksi automaattisen käynnistyksen sijasta, koska se voi olla suotuisampaa niiden palvelujen kannalta.

Huomioitavaa testauksesta

Kokonaisuudessaan testaus osoittautui paljon asennusosuutta sujuvammaksi toteuttaa, eikä suurempiin ongelmiin törmätty. Suoraviivaisen testausprosessin ansiosta testaus sujui vaihe kerrallaan. Aina kun palautussuunnitelma suoritetaan, kannattaa muistaa ajaa myös sen reprotect-toiminto, koska tätä ennen uusia palautuksia ei voi tehdä. Testauksessa kannattaa kiinnittää myös huomiota palautussuunnitelman ja sen reprotect-toiminnon ajamisen yhteydessä, että palautussuunnitelman toimivuus testataan.

5.4 Yhteenveto

Käytännön osuudessa tuli vastaan ongelmia erityisesti testiympäristön asennusvaiheessa. Ongelmista kuitenkin selvittiin ja testiympäristö saatiin pystytettyä ja testattua onnistuneesti. Apuna asennuksissa ja testauksen toteuttamisessa olivat VMwaren viralliset asennus- ja arviointioppaat.

Ohjelmistojen oikeaoppinen asennus ja määritys veivät useita viikkoja aikaa, mutta se olisi nykytietämyksellä mahdollista tehdä viikossa valmiiksi. Testauksen

osalta prosessi oli varsin nopea, ja palautussuunnitelman sekä siihen liittyvien toimintojen testaus suoritettiin yhden päivän aikana. Vaikka pienen suojattavan kokonaisuutensa vuoksi palautussuunnitelman ajo kesti vain noin tunnin, voi kyseinen aika vaihdella sen mukaan, kuinka suuresta virtuaalikoneiden kokonaisuudesta on kyse ja kuinka tehokas konesaliympäristö on käytössä. Esimerkiksi parin kymmenen virtuaalikoneen käsittely olisi useamman tunnin prosessi hieman isommassa ympäristössä.

6 POHDINTA

Konesalin peilaus jo käsitteenä oli opinnäytetyöhön lähdettäessä epämääräinen, joten en voi sanoa tämän aihepiirin olleen lähelläkään omaa mukavuusaluetta. Muun muassa aiheeseen keskeisesti liittyvät disaster recovery ja replikointi olivat uusia asioita, joita ei kursseilla ollut ikinä edes käsitelty. Pitkän alustavan taustatutkimuksen jälkeen aiheeseen ja siihen liittyviin osasiin pääsi kuitenkin pikku hiljaa sisälle ja teoriaosuuden teko lähti liikkeelle.

Opinnäytetyön aihe oli tiedossa pitkään, joten aiheeseen oli aikaa perehtyä ennen käytännön työtä. Tämä ei kuitenkaan valmistanut siihen, mistä konesalin peilausympäristö oikeasti koostuu, joten aiheeseen täytyi perehtyä käytännön osuuden rinnalla myös paljon yksityiskohtaisemmalla tasolla yleisten ideoiden ja käsitteiden lisäksi. Käytännön osuus ei lähtenyt ongelmitta liikkeelle, sillä Site Recovery Manageria varten suunniteltu fyysinen ympäristö koki muutoksia sen sijainnin ja rakenteen suhteen useaan otteeseen. Tämä jätti aikaa perehtyä aiheeseen, ja niinpä opinnäytetyön teoriaosuus muotoutui ennen käytäntöä.

Alustavasti konesaliympäristöt oli tarkoitus toteuttaa siten, että Site Recovery -ympäristöt olisivat sijainneet oikeasti maantieteellisiltä sijainneiltaan eri paikoissa. Opinnäytetyön aiheen saadessani suunnittelutyötä verkon topologian osalta ja alustavia asennustöitä kerettiin tehdä, mutta harmikseni tilanne muuttui. Tämä oli opinnäytetyön osalta suurin pettymys.

Aikataulujen suhteen tuli itse käytännön työssä ongelmia, kuten jo asennus- ja testiosiossa kerrottiin. Tämä ei ollut yhtään odotettavissa työhön ryhdyttäessä, sillä olin jopa aikataulullisesti varannut ympäristön asennukseen vain kaksi viikkoa. Kyseinen vaihe kestikin yli kuukauden, mutta sain aikataulua kiinni tekemällä muita vaiheita kuten teoriaa ja dokumentointia siinä sivussa silloin, kun käytäntö tökki.

Työssä ei varsinaisesti käsitelty kaikkia teorian osa-alueita, vaikka palautussuunnitelmaa sekä replikointia toteutettiinkin omassa mittakaavassaan. Tein näin,

koska katsoin niiden olevan aiheen nähden tärkeitä ideoita ymmärtää, tavoitteena lukijan hahmottavan käytännön ympärillä olevaa kokonaisuutta paremmin.

Kokonaisuudessaan tämä työ oli hyppy tuntemattomaan. Oletukseni osoittautuivat niin käytännön kuin myös teorian suhteen melko erilaisiksi. Vastoinkäymisiä tuli vastaan usein, mutta sinnittelin tästä huolimatta esimerkiksi käytännön asennusten suhteen, kun aikataulut venyivät eikä ratkaisuista ollut päivien etsinnän jälkeen aavistustakaan. Lopulta Site Recovery Manager -ympäristön toimivuutta päästiin testaamaan ja se todettiin täysin toimivaksi ratkaisuksi konesalien peilauksessa.

LÄHTEET

Avamar. 2014. EMC AVAMAR. Dedublication backup software and system. Viitattu 3.7.2015. http://finland.emc.com/collateral/software/data-sheet/h2568-emc-avamar-ds.pdf

CIO. 2009. Data Center Definition and Solutions. Viitattu 2.6.2015. http://www.cio.com/article/2425545/data-center/data-center-definition-and-solutions.html

DELL. 2014a. AppAssure datasheet. Viitattu 16.2.2015. http://software.dell.com/documents/appassure-datasheet-30207.pdf

DELL. 2014b. Dell AppAssure Replication. Viitattu 2.7.2015. http://software.dell.com/documents/dell-appassure-replication-technicalbrief-29890.pdf

DELL. 2014c. AppAssure Backup, Repication and Recovery. Viitattu 1.7.2015. http://software.dell.com/products/appassure/

EMC. 2014. RecoverPoint Data Sheet. Viitattu 19.2.2015. http://www.emc.com/collateral/software/data-sheet/h2769-recoverpoint-ds.pdf

Fritsch, Nick. 2014. EMC Recoverpont for VMS. Viitattu 1.7.2015. http://vmnick.com/2014/08/26/emc-recoverpoint-for-vms/

Gsoedl, Jacob. 2011. TechTarget. Array-based and network-based replication. Viitattu 20.3.2015. http://searchdisasterrecovery.techtarget.com/tip/Data-replication-strategies-Array-based-and-network-based-replication¨

Iivari, Mika & Laaksonen, Mika. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Helsinki, Finland: Tietosanoma Oy.

Palo Alto Networks. 2015. What is a data center? Viitattu 4.6.2015. https://www.paloaltonetworks.com/resources/learning-center/what-is-a-data-center.html

Posey, Brien. 2012. TechTarget. Hypervisor-based replication vs. traditional replication. Viitattu 25.3.2015. http://searchdatabackup.techtarget.com/answer/Hypervisor-based-replication-vs-traditional-replication

Rouse, Margaret. 2012a. TechTarget. Array-based replication. Viitattu 25.3.2015. http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication

Rouse, Margaret. 2012b. TechTarget. Host based replication. Viitattu 25.3.2015. http://searchstorage.techtarget.com/definition/Host-based-replication

Ruest, Danielle & Ruest, Nelson. 2009. Virtualization: a beginner's guide. USA: The McGraw-Hill Companies.

Seagrave, Simon. 2012. What is VMware's vSphere 5.1 VDP Backup Solution? Viitattu 3.7.2015. http://www.datacenterinsiders.com/what-is-vmwares-vsphere-5-1-vdp-backup-solution/

Spectra. 2011. Three Key Requirements of a Sound Disaster Recovery Strategy. Viitattu 13.4.2015. https://www.spectralogic.com/index.cfm?fuseaction=home.displayFile&DocID=3664

Staimer, Mark. 2014. TechTarget. How frequently should you conduct failover testing? Viitattu 25.3.2015. http://searchdisasterrecovery.techtarget.com/answer/How-frequently-should-you-conduct-failover-testing

Varghese, Mathew. 2002. Disaster Recovery. Boston, MA, USA: Course Technology.

Veeam. 2013. The Countdown continues: Introducing the Veeam vSphere Web Client Plug-In. Viitattu 9.7.2015. http://www.veeam.com/blog/the-countdown-continues-introducing-the-veeam-vsphere-web-client-plug-in.html

Veeam. 2015. Availability for the Modern Data Center. Viitattu 3.7.2015. http://www.veeam.com/data-center-availability-suite.html

VMware. 2015a. vCenter Site Recovery Manager. Viitattu 7.2.2015. https://www.vmware.com/products/site-recovery-manager/features.html

VMware. 2015b. Overview of VMware vCenter Site Recovery Manager. Viitattu 1.7.2015. http://pubs.vmware.com/srm-60/index.jsp#com.vmware.srm.install_config.doc/GUID-C1E9E7D0-B88F-4D2E-AA15-31897C01AB82.html

VMware. 2015c. VMware vCenter Site Recovery Manager 6.0 Evaluation Guide. Viitattu 1.7.2015. https://www.vmware.com/files/pdf/products/SRM/VMware-vCenter-Site-Recovery-Manager-Evaluation-Guide.pdf

Vmware. 2015d. Data Protection. Viitattu 3.7.2015. http://www.vmware.com/products/vsphere/features/data-protection

Wallen, Jack. 2013. TechRepublic. 10 benefits of virtualization in the data center. Viitattu 3.6.2015. http://www.techrepublic.com/blog/10-things/10-benefits-of-virtualization-in-the-data-center/